LEXOLOGY
Getting The Deal Through

FINTECH 2024

Contributing editors
Angus McLean and Oliver Irons

This publication is intended to provide general information on law and policy. The information and opinions it contains are not intended to provide legal advice, and should not be treated as a substitute for specific advice concerning particular situations (where appropriate, from local advisers).

Enquiries concerning reproduction should be sent to customersuccess@lexology.com. Enquiries concerning editorial content should be directed to the Content Director, Clare Bolton – clare.bolton@lbresearch.com.

LEXOLOGY
Getting The Deal Through

START READING

© Law Business Research Ltd 2023

Jurisdictions

Introduction 1
Angus McLean, Oliver Irons and Gordon Ritchie
Simmons & Simmons

Australia 4
John Bassilios
Hall & Wilcox

Belgium 28
Jérémie Doornaert, Martin Carlier, Ellen Herinckx and Raf Thielemans | Simmons & Simmons
Marc De Munter | Baker Tilly

Bulgaria 55
Damian Simeonov, Nikolay Zisov, Svetlina Kortenska, Georgi Drenski and Stela Sabeva
Boyanov & Co

Canada 80
Alix d'Anglejan-Chatillon, Ramandeep Grewal, David Elder, Shawn Smith and Éric Lévesque
Stikeman Elliott LLP

China 103
Jingyuan Shi, Yuchen Lai and Yanyu Lai
Simmons & Simmons

Denmark 128
Rasmus Mandøe Jensen and Jónas Már Torfason
Plesner Advokatpartnerselskab

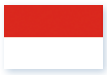
Egypt 151
Mohamed Hashish and Farida Rezk
Soliman, Hashish & Partners

Germany 169
Christopher Götz, Daniel Kendziur, Jochen Kindermann, Sascha Kuhn and Sascha Morgenroth
Simmons & Simmons

Greece 198
Alexandra Th Kondyli, Nikos Askotiris, Eleana Rouga, Maria Chronaki, Dimitris Passas, Dimitra Karampela, Anna Pechlivanidi and Sergios Charalambous
Karatzas & Partners Law Firm

Hong Kong 219
Jolyon Ellwood-Russell, Michelle Ta, Donia Chu and Galvin Chua
Simmons & Simmons

India 242
Probir Roy Chowdhury, Yajas Setlur, Kumarmanglam Vijay, Pratish Kumar and Nikhil George
JSA



Indonesia 265
Winnie Yamashita Rolindrawan, Ruth M Ginting and Farrah Azizah Habibie
SSEK Law Firm

Ireland 284
Ian O'Mara and Joe Beashel
Matheson LLP

Italy 303
Benedetta Noro, Gabriella Rubino, Guendalina Catti de Gasperi, Marco Graziani and Marco D'Agostini
Legance

Japan 329
Ken Kawai, Akihito Miyake, Yutaka Shimoo and Kensuke Inoue
Anderson Mōri & Tomotsune

Luxembourg 349
Cathrine Foldberg Møller, Julie Carbiener, Camille Saettel, Camille Bénézet and Maya Coumes
Simmons & Simmons

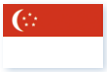
Malta 370
Leonard Bonello and James Debono
Ganado Advocates

Netherlands 390
Jeroen Bos, Koen van Leeuwen and Marise Kok
Simmons & Simmons

Published July 2023

New Zealand 424
Derek Roth-Biester and Megan Pearce
Anderson Lloyd

Nigeria 441
Ugochukwu Obi, Tare Ologun, Omolade Afonja, Adesola Baruwa and Anthony Obidike
Perchstone & Graeys



Singapore 458
Ying Wang and Ashleigh Low
Simmons & Simmons

South Korea 483
Juho Yoon, Young Ju Park, Se Yeong Im and Jinhee Rhew
Bae, Kim & Lee LLC

Spain 504
Carmen Torres, Ignacio González, Juan Sosa, María Tomillo and Raquel Ballesteros
Simmons & Simmons

Sweden 530
Emma Stuart-Beck, Nicklas Thorgerzon, Caroline Krassén and Anton Sjökvist
Vinge

Switzerland 551
Luca Dal Molin, Daniel Haeberli, Stefan Oesterhelt, Richard Stäuber, Manuel Baschung and Alexander Wherlock
Homburger

Taiwan 573
Abe T S Sung and Eddie Hsiung
Lee and Li Attorneys at Law

Turkey 598
Cigdem Ayozger Ongun and Deniz Erkan
SRP Legal

United Arab Emirates 629
Raza Rizvi and Muneer Khan
Simmons & Simmons

United Kingdom 661
George Morris, Oli Ward, Sophie Sheldon, Olly Jones and Gordon Ritchie
Simmons & Simmons

United States 706
Casey J Jennings, Paul T Clark, Jeffrey M Berman, Beth H Alter and Seth Kuntz
Seward & Kissel LLP

Vietnam 732
Le Thi Loc, Ha Nguyen Nhat Minh, Ho Ngoc Quynh Anh, Ta Nguyen Nhu Quynh and Ngo Thi Khanh Linh
YKVN

Published July 2023

Introduction

Angus McLean, **Oliver Irons** and **Gordon Ritchie**
Simmons & Simmons

RETURN TO CONTENTS

What's old is new

With the excitement surrounding the potential for financial technology to change the world and transform lives over the past few years, it is worth remembering that financial innovation has been with us for some time. From the invention of money before the beginning of written history, to the advent of the double-entry accounting method in Korea during the Goryeo dynasty and its adoption by the Medici family in the 14th century, fintech has come a long way.

However, in recent years it has been difficult to open a newspaper (or a news aggregator) without reading about the promise of artificial intelligence (AI), distributed ledger technology, cloud computing, and ever-cheaper computer power.

Combined with the creation of new business models, the increasing democratisation of technical education, significant investment, and public policy and regulatory support, the fintech sector has experienced remarkable growth over the past 10 years. Although policy and regulatory attitudes towards some areas of the sector have chilled significantly in the past few years, it is still an exciting time to be a fintech-focused entrepreneur, financier, investor, policy maker, technologist, or (whisper it quietly) lawyer.

A broad church

You know that fintech has penetrated the public consciousness when the portmanteau enters the dictionary for the first time. Merriam-Webster defined fintech as 'products and companies that employ newly developed digital and online technologies in the banking and financial services industries'. It should be clear from this definition that fintech is a broad church. It encompasses businesses of all sizes, from the founder writing the first lines of code to some of the largest and most valuable companies in the world. It also encompasses a wide variety of technologies and business models. Fintech products and services now exist across the entire financial services sector, including:

- payments processing and networks;
- cryptoassets;
- mobile wallets and remittances;
- retail investing and secondary markets;
- capital markets and institutional trading;
- core banking and infrastructure;
- wealth management;
- personal finance and savings through deposit aggregators;

Read this article on Lexology

- digital banking;
- real estate lending and investing;
- financial regulation and compliance;
- insurance;
- payroll and benefits;
- credit scores and analytics; and
- personal and business lending.

While there are significant differences between the legal issues affecting businesses operating across this diverse universe of sub-sectors, this publication seeks to address the most pressing issues that we see in our day-to-day practice, advising firms in all of these areas.

Regulatory headwinds and policy support

For a relatively young industry that, until recently, has only ever enjoyed a largely supportive regulatory and policy environment and enthusiastic investors, there has been a marked change in direction of the prevailing winds around the fintech sector over the past 24 months.

Some fintech businesses and products are now of sufficient scale and importance that they have the ability to impact significant numbers of consumers and cause systemic risks to the financial system. In addition, recent developments in the fintech industry, such as high profile corporate failures – particularly in the embedded payments and finance space – enforcement actions and regulatory investigations into key players in the market have marked a further toughening of the attitude of many policymakers and regulators to the level of support afforded to, and their oversight of, fintech companies. The new Virtual Assets and Related Regulated Activities Regulation in Dubai and the Markets in Crypto Assets Regulation in Europe are examples of regulators' attempts to regulate the ever-expanding mosaic of businesses operating in the cryptoassets space, while striking a delicate balance between supporting innovation and ensuring a secure financial system.

Ironically, this tightening of the regulatory perimeter around cryptoassets, coincides with a marked uptick in the level of activity around the world, from governments, central banks, regulators, traditional financial institutions and investors, investigating how the distributed ledger technology that underpins the cryptoassets industry can be leveraged to launch central bank digital currencies (CBDCs), or revamp the wholesale payments systems. The International Monetary Fund recently reported that over 100 countries are exploring the use of retail CDBCs.

While not always cited as essential to these developments, distributed ledger technology has also been identified as a key innovation that could transform the operation of the capital markets as evidenced by various initiatives, including the EU DLT Pilot Regime, the UK Financial Markets Infrastructure sandbox, the Singapore FinTech Regulatory Sandbox and the China Fintech Development Plan, among others. All of these programmes are designed to remove some of the legal and regulatory hurdles potentially preventing firms building, operating and using distributed ledger technology to replace aspects of the existing financial markets technology infrastructure.

Another significant development over the past 12 months has been the explosion of interest in AI across all industries. The fintech sector is no exception. Over the next 12 months, we

Read this article on Lexology

expect the heightened focus on AI to impact the fintech landscape increasingly, especially in light of the forthcoming AI-specific regulatory changes in Europe, China and other regions. Those new regulatory regimes will add yet another regulatory burden for fintech firms to understand and navigate.

In all of these areas, businesses need to understand the way in which they may be impacted by the changes in the nature of the legal and regulatory controls to which they are subject.

Fintech 2024

This publication is intended to provide a user-friendly resource to help fintech entrepreneurs and their advisers and investors around the world navigate the often complex key legal and regulatory issues on which we are most often asked to advise.

Now, more than ever, understanding the legal and regulatory landscape in which you operate is paramount to success. We hope this edition serves as a valuable reference point wherever you are on your fintech journey.

simmons+simmons

Angus McLean	angus.mclean@simmons-simmons.com
Oliver Irons	oliver.irons@simmons-simmons.com
Gordon Ritchie	gordon.ritchie@simmons-simmons.com

Citypoint, 1 Ropemaker Street, London EC2Y 9SS, United Kingdom
Tel: +44 20 7628 2020
www.simmons-simmons.com

Read more from this firm on Lexology

Read this article on Lexology

Australia

[John Bassilios](#)
Hall & Wilcox

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 5
General innovation climate 5
Government and regulatory support 6

FINANCIAL REGULATION 6
Regulatory bodies 6
Regulated activities 7
Consumer lending 8
Secondary market loan trading 8
Collective investment schemes 9
Alternative investment funds 9
Peer-to-peer and marketplace lending 10
Crowdfunding 10
Invoice trading 10
Payment services 10
Open banking 11
Robo-advice 11
Insurance products 12
Credit references 12

CROSS-BORDER REGULATION 12
Passporting 12
Requirement for a local presence 13

SALES AND MARKETING 13
Restrictions 13

CRYPTOASSETS AND TOKENS 14
Distributed ledger technology 14
Cryptoassets 14
Token issuance 15

ARTIFICIAL INTELLIGENCE 15
Artificial intelligence 15

CHANGE OF CONTROL 16
Notification and consent 16

Read this article on Lexology

FINANCIAL CRIME 16

Anti-bribery and anti-money laundering procedures 16
Guidance 17

DATA PROTECTION AND CYBERSECURITY 17

Data protection 17
Cybersecurity 18

OUTSOURCING AND CLOUD COMPUTING 19

Outsourcing 19
Cloud computing 19

INTELLECTUAL PROPERTY RIGHTS 20

IP protection for software 20
IP developed by employees and contractors 20
Joint ownership 21
Trade secrets 21
Branding 22
Remedies for infringement of IP 22

COMPETITION 23

Sector-specific issues 23

TAX 23

Incentives 23
Increased tax burden 24

IMMIGRATION 25

Sector-specific schemes 25

UPDATE AND TRENDS 26

Current developments 26

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Financial technology innovations in Australia are rapidly accelerating and are competitive in a global context. Australia's national fintech association, FinTech Australia, estimates that the fintech industry in Australia is worth A$4 billion. The covid-19 pandemic has bolstered the strength of the fintech market as increased online transactions during lockdowns led to more businesses requiring digital payment capabilities. The Australian Trade and Investment Commission attributes the success of fintech in Australia to a supportive regulatory environment, a highly qualified and diverse talent pool, our geographic proximity to Asia and desire of Australian fintech companies to expand their international reach.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Government bodies and regulators in Australia are eager to support fintech innovations without comprising the principles of existing regulations. Forms of support offered by government bodies and regulators include:

- an innovation hub launched by Australian Securities and Investment Commission, which allows fintech businesses to access informal assistance to navigate Australia's regulatory system;
- the enhanced regulatory sandbox (ERS). The ERS has been available since 1 September 2020 and allows businesses to test their financial services or credit activities before obtaining an Australian financial services licence or Australian credit licence for a period of up to 24 months. To access the ERS exemption, businesses must satisfy the eligibility requirements and conditions for entry; and
- establishment of fintech bridges with the United Kingdom and Singapore. The purpose of a fintech bridge is to improve access for Australian fintech businesses into the UK and Singapore markets, including entry into regulatory sandboxes, quicker licence processing and facilitating advice and mentorship opportunities for Australian fintech businesses.

Government bodies continually review aspects of the fintech industry to strengthen the regulatory environment, with a particular focus on ensuring regulatory settings are fit for purpose.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

The key regulatory bodies in Australia include:

- the Australian Securities and Investment Commission (ASIC);
- the Australian Prudential Regulation Authority (APRA);
- the Australian Transaction Reports and Analysis Centre (AUSTRAC);
- the Reserve Bank of Australia (RBA); and
- the Australian Competition and Consumer Commission (ACCC).

Each regulatory body performs a different function and a fintech business may need to interact with more than one regulatory body for the provision of its products and services.

ASIC regulates financial services, consumer credit and authorised financial markets. It is responsible for licensing and monitoring businesses that engage in financial services or consumer credit activities. Entities cannot engage in certain activities without an Australian financial services licence or Australian credit licence (unless an exemption

applies). Licensees must comply with their obligations under the law and the conditions of their licence.

APRA is responsible for the prudential regulation and supervision of banking, insurance and superannuation institutions to promote financial system stability. Its role involves authorising entities to be banking or insurance businesses or to be a trustee of a superannuation fund.

AUSTRAC is responsible for preventing, detecting and responding to criminal abuse of the financial system. Industries regulated by AUSTRAC include banking, digital currency exchanges and financial services providers. Entities regulated by AUSTRAC are required to have an anti-money laundering or counter-terrorism financing programme and comply with ongoing reporting obligations.

RBA is the central bank of Australia and is responsible for maintaining the stability of the financial system. As the primary payments system regulator, the RBA ensures that the payments system is safe and robust. RBA may designate a particular payment system as being subject to its regulation and determine rules for participating in that system.

ACCC is the regulator of competition and national consumer law in Australia, including enforcing prohibitions on misleading and deceptive conduct and unconscionable conduct. The scope of ACCC's regulation includes all businesses.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Financial services and credit activities trigger licensing requirements in Australia unless an exemption applies. Fintech businesses testing innovative financial services or credit activities may benefit from the enhanced regulatory sandbox exemption if it meets the eligibility criteria.

Australian financial services licence

Fintech businesses carrying on a financial services business in Australia must hold an Australian financial services licence (AFSL). Financial services include the provision of financial product advice, dealing in financial products, making a market for financial products, operating registered schemes, providing custodial or depository services and operating a crowdfunding service. A financial product is a facility through which, or through the acquisition of which, a person makes a financial investment, manages financial risk or makes non-cash payments. Australian financial services licensees must comply with obligations under the Corporations Act and Corporations Regulations.

Australian credit licence

Fintech businesses providing consumer credit activities in Australia must hold an Australian credit licence (ACL). Credit activities include providing credit under, suggesting or assisting with, a credit contract or consumer or consumer lease. Australian credit licensees must comply with their obligations under the National Consumer Credit Protection Act 2009, National Credit Code and National Consumer Credit Protection Regulations 2010.

Read this article on Lexology

APRA-regulated entities

Banking (including stored value facilities), insurance and superannuation businesses are required to be licensed by APRA. Licensed entities are required to meet APRA's prudential standards.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

ASIC regulates consumer lending pursuant to the National Consumer Credit Protection Act (NCCP Act), the National Credit Code (NCC) and National Consumer Credit Protection Regulations. Under the NCCP Act, persons engaging in a credit activity must hold an ACL, unless an exemption applies. The purpose of the NCCP Act is to provide protections to consumers and impose obligations on creditors in providing consumer credit.

Licensees must comply with responsible lending conduct obligations in the NCCP Act, which prevents Australian credit licensees from entering into a credit contract with a consumer, suggest a credit contract to a consumer or assist a consumer to apply for a credit contract if it is unsuitable. ASIC's views on responsible lending obligations are set out in Regulatory Guide RG 209.

Banks carrying out consumer lending activities are also required to comply with APRA's lending standards.

Further, the buy now, pay later (BNPL) industry has gained traction in Australia, but not without additional suggestions for further regulation. In November 2022, the Treasury released a consultation paper outlining three broad options for regulatory intervention:

- strengthening the industry code for BNPL;
- creating tailored legislation under the Credit Act; or
- creating full regulation under the Credit Act.

In May 2023, the government announced that BNPL will be regulated through the second option, meaning that BNPL service providers will need to hold an Australian credit licence and comply with the relevant obligations. ASIC will continue to regulate this.

Secondary market loan trading

6 | Are there restrictions on trading loans in the secondary market in your jurisdiction?

There are no legislative restrictions to trading loans in the secondary market. The main restriction on trading loans is the limited secondary market in Australia.

The trading of consumer loans regulated under the National Consumer Credit Protection Act will require assignees of the loan to hold an Australian credit licence.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Collective investment schemes typically fall within the meaning of a 'managed investment scheme' (MIS) under the Corporations Act. A MIS has the following features:

- people contribute money or money's worth as consideration to acquire interests to benefits produced by the scheme (whether the rights are actual, prospective or contingent and whether they are enforceable or not);
- any of the contributions are to be pooled, or used in a common enterprise, to produce financial benefits or benefits consisting of rights or interests in property for the members who hold interests in the scheme (whether as contributors to the scheme or as people who have acquired interests from holders); and
- the members do not have day-to-day control over the operation of the scheme (whether or not they have the right to be consulted or to give directions).

Responsible entities and fund operators of an MIS are typically required to hold an AFSL. Registered MIS are subject to additional obligations under Chapter 5C of the Corporations Act. The meaning of a MIS is broad and could encompass many schemes not otherwise viewed as collective investments; however, a recent case *LCM Funding Pty Ltd v Stanwell Corporation Limited* [2022] FCAFC 103 highlighted the overarching purpose of the regime should be taken into account in concluding whether a scheme is a MIS.

The Corporate Collective Investment Vehicle (CCIV) regime commenced on 1 July 2022. A CCIV is a type of company limited by shares that is an investment vehicle. The CCIV regime incorporates some aspects of the existing regulatory framework for MIS but has additional features such as the ability to operate 'sub-funds'.

Depending on the structure of the offering, fintech companies providing alternative finance products or services could fall within the scope of a MIS. ASIC information sheet INFO 213 provides guidance on marketplace lending schemes structured as an MIS.

Equity-based crowd-sourced funding is governed under Part 6D.3A of the Corporations Act. Crowdfunding platforms that fall within the scope of Part 6D.3A are specifically excluded from the definition of a MIS.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Collective investment undertakings that raise capital from a number of investors and invest it in accordance with a defined investment policy will generally satisfy the elements of a managed investment scheme if investors have no day-to-day control over the operation of the scheme. Managers of a managed investment scheme are required to hold an Australian financial services licence. If interests in the scheme are offered to retail investors, the scheme must be registered with ASIC and must have a constitution and compliance plan

that meet various requirements. In addition, a Target Market Determination and a Product Disclosure Statement (similar to a prospectus) needs to be prepared.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

While there is no specific regulation, aspects of peer-to-peer or marketplace lending may give rise to regulatory requirements. For example, if the lending scheme is structured as a managed investment scheme, the operator would be required to hold an Australian financial services licence. Where the lending relates to consumer credit, an Australian credit licence is required. ASIC provides its guidance on marketplace lending products and the applicable regulations in information sheet INFO 213.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

The Corporations Act provides a crowd-sourced funding (CSF) regime that allows companies to make public offers of shares with reduced regulatory requirements. ASIC released RG 261 to provide guidance to companies seeking to raise funds through equity-based CSF, including eligibility to make an offer under the CSF regime and obligations of the company.

Providers of CSF services are required to hold an AFSL. ASIC's RG 262 provides guidance on the AFSL obligations and specific CSF regime obligations applicable to intermediaries seeking to provide CSF services.

Invoice trading

11 Describe any specific regulation of invoice trading in your jurisdiction.

Some invoice factoring arrangements could technically satisfy the definition of a 'derivative' in section 761D of the Corporations Act. ASIC issued legislative instrument ASIC Corporations (Factoring Arrangements) Instrument 2017/794 to relieve debt factoring arrangements from the requirement to hold an AFSL.

Payment services

12 Are payment services regulated in your jurisdiction?

The RBA is the primary payments system regulator however the scope of RBA's designation power is unlikely to extend to all new fintech innovations (for example, intermediaries such as digital wallets may not be captured).

ASIC is responsible for the licensing and regulation of non-cash payment facility providers.

APRA, ASIC and RBA are responsible for the regulation of purchase payment facility (PPF) providers.

Read this article on Lexology

PPFs that are widely available and redeemable upon demand into Australian currency are considered to carry on a banking business and require a special class of authorised deposit-taking institution authorisation from APRA, which licenses a limited range of banking activities. If PPFs are not widely available nor redeemable for Australian currency, they may be either authorised or exempted by the RBA. Depending on the nature of the PPF, it may also constitute a non-cash payment facility that could require an Australian financial services licence.

Payment services businesses may also voluntarily subscribe to be bound by the ePayment Code administered by ASIC.

In June 2023, the Treasury provided direction as to its key priorities for modernising payments and simplifying processes of obtaining different authorisations, in particular proposing that ASIC is the single point of contact for applications of all sorts of authorisations.

It is also noted that BNPL services have attracted the need for additional regulation, requiring BNPL service providers will need to hold an Australian credit licence and comply with the relevant obligations. This too, is currently regulated by ASIC.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

In November 2017, the government introduced consumer data right (CDR) in Australia, which seeks to provide consumers with greater access and control over their data. ACCC is the lead regulator for CDR and is responsible for its development and implementation.

The first sector of CDR is open banking, which has allowed bank customers to provide accredited third parties with savings, credit card, mortgage, personal loan and joint bank account data since late 2020. Accredited businesses could include other authorised banks, financial institutions and organisations.

Australia is still in the early stages of adopting an open banking initiative, meaning that the incorporation of the CDR regime in Australia has been slow.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

ASIC defines robo-advice as the provision of automated financial product advice using algorithms and technology without the direct involvement of a human adviser. ASIC released RG 255 highlighting issues associated with providing digital advice to retail clients. In summary, if the robo-adviser provides customers with general or personal financial product advice, it will need to hold an Australian financial services licence (AFSL). If the robo-adviser is limited to providing factual information, generally an AFSL is not required.

Read this article on Lexology

Where the robo-adviser is used to provide a designated service under anti-money laundering or counter-terrorism financing legislation, it may have reporting obligations to AUSTRAC.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Generally, life insurance or general insurance businesses (issuers) are required to be authorised by APRA and to hold an Australian financial services licence, whereas non-insurance businesses that sell or market insurance products are only required to hold an AFSL.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Under the Privacy Act, only credit reporting agencies are permitted to collect and provide consumer credit information to credit providers.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

FFSP exemptions

Foreign financial services providers (FFSP) may qualify for relief from the requirement to hold an Australian financial services licence (AFSL).

- An FFSP may be exempted from holding an AFSL if it only provides funds management financial services to certain types of professional investors in Australia.
- An FFSP that is authorised by an overseas regulatory authority alternatively may be eligible to apply for a modified form of an AFSL (known as a foreign AFS licence) to provide specified financial services to wholesale clients only. Where an FFSP obtains a foreign AFS licence, it is exempted from certain obligations under Chapter 7 of the Corporations Act, provided they are subject to sufficiently equivalent overseas regulatory requirements.

Australian Securities and Investment Commission (ASIC) RG 176 provides guidance on the eligibility requirements for FFSPs and the obligations that apply. The current relief for FFSPs is expected to apply until 31 March 2024.

In February 2022, the government introduced the Treasury Laws Amendment (Streamlining and Improving Economic Outcomes for Australians) Bill 2022 seeking to restore regulatory relief for FFSPs. This bill has not yet been passed and lapsed in April 2022. We note, however, that following the lapse of the Bill, ASIC has extended the transitional relief for an

additional year (to 31 March 2024) as mentioned above. FFSPs can therefore rely on regimes being either the sufficient equivalence or limited connection relief until this date.

Once this transitional relief expires, it is unclear what the permanent options will be in future. This depends on whether the Bill is reintroduced into Parliament, and passed.

Foreign passport funds

In 2018, Australia committed to the Asia Region Funds Passport, which aims to remove unnecessary regulatory barriers and allows collective investment schemes in a participating economy to market their products in Australia. The process requires the foreign passport fund to register as a foreign country in Australia, satisfy an 'ongoing offer' requirement in its home country, lodge a notice of intention to offer interests in Australia with ASIC and provide ASIC with a PDS for the fund. Parties to the Asia Region Funds Passport include Australia, New Zealand, Japan, South Korea and Thailand. ASIC's RG 138 concerning foreign passport funds outlines the entry and ongoing requirements for 'notified foreign passport funds'.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

It is possible for a fintech company to obtain an AFSL in Australia where it is registered as a foreign company and carries on a business in Australia.

It could be onerous to register as a foreign company as they required to maintain a registered office in Australia that opens each business day from at least 10am to 12pm and 2pm to 4pm with a representative present during business hours and meet certain financial reporting obligations.

Due to the conditions attached to registering a foreign company, it may be more convenient for foreign fintech companies to incorporate an Australian resident subsidiary company to hold the AFSL.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

The marketing of a financial product constitutes a financial service that requires an Australian financial services licence. Australian Securities and Investment Commission RG 234 contains good practice guidance on advertising financial products and services.

The Australian Securities and Investment Commission Act 2001 and Corporations Act provides consumer protection in relation to financial services and products to ensure that promoters do not make false or misleading statements or engage in misleading or deceptive

conduct. The Corporations Act requires marketing material to include the identity of the issuer and to state that a PDS is available and that a person should consider the PDS in deciding whether to acquire the product.

For Australian credit licensees, marketing material for credit products must comply with the National Consumer Credit Act, which includes the requirement to include the Australian credit licence number on all printed advertisements.

All businesses are subject to the overarching obligations under the Australian Consumer Law, which requires businesses not to mislead or deceive consumers or other businesses.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

Australian Securities and Investment Commission (ASIC) released information sheet INFO 219 for businesses using distributed ledger technology or blockchain. In ASIC's view, the existing regulatory framework accommodates the current distributed ledger technology use cases.

Digital currency exchange providers are required to register with the Australian Transaction Reports and Analysis Centre (AUSTRAC); and comply with anti-money laundering (AML) and counter-terrorism financing (CTF) rules and regulations.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

The applicable rules and regulations depend on whether the cryptoasset is a financial product. If the cryptoasset is a financial product, then any business that involves issuing, advising and dealing in the cryptoasset would require an Australian financial services licence (AFSL).

The promotion of financial services and products requires an AFSL and is subject to consumer protection rules under the ASIC Act and Corporations Act to ensure that promoters to do not make false or misleading statements or engage in misleading or deceptive conduct.

Where the use of cryptoassets involves a digital currency exchange, the entity is required to register with AUSTRAC and comply with AML and CTF rules and regulations.

ASIC has also released INFO 225, which discusses the obligations under the Corporations Act 2001 relating to promotional communications about crypto-assets or ICOs. This mainly

is ensuring that these communications are not misleading or deceptive, and that they do not contain false information, consistent with Australia's consumer laws and protections.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

There is no specific rules or regulations governing the issuance of tokens however ASIC information sheet INFO 225 discusses implications of token issues under the Corporations Act, ASIC Act and Australian Consumer Law.

If the tokens meet the definition of a financial product, then the token issue and offer is a financial service that requires an Australian financial services licence. If the token represents a share in a body corporate then an AFSL is not required but a prospectus is required if the offer us made to retail clients.

We note that the Treasury has also released in February 2023, a token mapping consultation paper. The consultation paper suggests that tokens, token systems, as well as its functions (benefits received from a token system such as payment) could be subject to regulation. Particularly in relation to intermediated token systems. The Treasury considered these sorts of assets to be defined as crypto assets given the link here is created through agreement. The paper highlights room for regulatory change being:

- crypto tokens tradeable on secondary markets cannot enforce rights against an issuer as the subsequent holder holds no rights against the original issuer;
- difficulties in being able to identify the issuer who is responsible for obligations relating to a particular crypto asset; and
- there is a lack of transparency of the underlying terms of an arrangement that links a crypto token to its asset, making it challenging for holders to exercise rights and for regulators to be able to determine whether the asset is a financial product.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

There are no specific regulations governing the use of artificial intelligence (AI). At the beginning of June of this year, the Australian government has released two papers discussing the importance of implementing appropriate safeguards for technologies. The government's Safe and Responsible AI in Australia Discussion Paper canvasses existing regulatory and governance responses in Australia and overseas, identifies potential gaps and proposes several options to strengthen the framework governing the safe and responsible use of AI.

The Australian Securities and Investment Commission released RG 255 on providing digital advice to retail clients, which takes the view that provision of financial product advice through a robo-adviser requires an Australian financial services licence. Where the robo-adviser is used to provide a designated service under anti-money laundering and counter-terrorism financing legislation, there may be reporting obligations to Australian Transaction Reports and Analysis Centre.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Australian financial services licensees and Australian credit licensees must notify Australian Securities and Investment Commission (ASIC) on becoming aware of any change in control under the Corporations Regulations and National Consumer Credit Protections Regulations. There is no requirement to obtain approval from ASIC prior to a change in control.

All companies (regardless of whether they are regulated) are required to notify ASIC of a change to their register of members, share structure, directors or secretaries or a change to the ultimate holding company of a proprietary company.

There are no specific consent requirements associated with a change of control, subject to takeover prohibitions under the Corporations Act and regulatory policy.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

The Anti-Money Laundering/Counter-Terrorism Financing Act (AML/CTF Act) imposes obligations on entities providing 'designated services' to combat illegal financing activities. Designated services include:

- taking deposits;
- making a loan in the course of carrying on a lending business;
- remittance services;
- exchanging currency; and
- exchanging digital currency for fiat.

Entities providing designated services are required to enrol as a reporting entity with the Australian Transaction Reports and Analysis Centre (AUSTRAC), conduct know-your-customer identification, monitor and report on transactions and suspicious matters, have an

AML and CTF programme in place and submit compliance certificates to the Australian Securities and Investment Commission.

Bribery of foreign public officials and Commonwealth public officials is covered in federal criminal legislation, whereas bribery of State and Territory public officials and private individuals is criminalised under the respective State and Territory legislation.

As of 1 July 2023, the Australian government has established the National Anti-Corruption Commission (NACC). The NACC will be an independent Commonwealth agency that has the aim of detecting, investigating and reporting on serious or systemic corrupt conduct in the Commonwealth public sector.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

Digital currency businesses have been required to comply with anti-money laundering or counter-terrorism financing laws since April 2018. AUSTRAC released a guide to assist digital currency exchange businesses with preparing an implementing an AML and CTF programme. In April 2023, the Attorney General announced a public consultation on the proposed reforms for the abovementioned AML and CTF regime. As AUSTRAC is the only regulator of Digital Currency Exchanges, the proposed reforms would expand the regulation to a broader range of services, being:

- exchanges between one or more other forms of digital currency;
- transfers of digital currency on behalf of a customer;
- safekeeping or administration of digital currency; and
- provision of financial services related to offer and sale of digital currency.

The consultation also seeks feedback on the implementation of the FATF travel rule.

AUSTRAC releases a number of anti-financial crime guides, some of which may be relevant to fintech companies, including Preventing the Criminal Abuse of Digital Currencies released in April 2022.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

Most businesses are subject to the Privacy Act 1988 (Cth), which deals with the protection of personal information of individuals. The Privacy Act regulates (among other things) the processing and transfer of personal information both domestically and in cross-border transactions.

The Privacy Act applies to and regulates dealing with 'personal information', being information about an individual where the identity of the individual is apparent or can reasonably be ascertained. As a result, the use of anonymised or aggregated information can still be regulated by the Privacy Act (such as where the relevant individual can reasonably be identified).

Where a fintech business is regulated by Australian Prudential Regulation Authority (APRA) or the Australian Securities and Investment Commission, additional obligations regarding processing of data can apply, for example, under APRA prudential standards.

The anonymisation of personal data in a blockchain is not necessarily sufficient to comply with or avoid the need to comply with the Privacy Act. This is because, where the identifiers in the blockchain becomes linked to an individual, all of the transactions carried out on the blockchain ledger can be viewed publicly.

The National Blockchain Roadmap published by the government in February 2020 identified Privacy Act obligations as a key regulatory challenge for blockchain systems in Australia as there may not be a responsible party to seek remedy from once privacy has been breached and there may be no way to subsequently remove personal information from a blockchain ledger.

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

Fintech businesses holding an Australian financial services licence (AFSL) are obliged to have adequate risk management systems, including cybersecurity.

The Australian Securities and Investment Commission expects AFSL holders to:

- have appropriate frameworks, policies, resources and controls to manage cybersecurity risks;
- take advice from experts on the baseline standard of cybersecurity in the context of their operations; and
- ensure the advice is promptly and properly implemented and regularly audited.

APRA prudential standard CPS 234 requires regulated entities to:

- clearly define the information security-related roles and responsibilities of its board, senior management, governing bodies and individuals;
- maintain an information security capability commensurate with the size and extent of threats to its information assets;
- implement controls to protect its information assets commensurate with its criticality and sensitivity;
- undertake systematic testing and assurance regarding the effectiveness of implemented controls; and
- notify APRA of security incidents or information security weaknesses in certain circumstances.

Amendments to the Security of Critical Infrastructure Act 2018 (Cth) (SOCI) are now in effect. The changes broaden the scope of entities and assets caught by SOCI and may apply to some fintech business depending on the goods or services they offer, including reporting obligations of incidents and assets.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

While it is possible for Australian financial services licence (AFSL) and Australian credit licence (ACL) holders to outsource their functions, they cannot outsource their responsibilities as a licensee. The Australian Securities and Investment Commission's expectations for outsourcing are set out in RG 104 (in relation to AFSL) and RG 205 (in relation to ACL).

Australian Prudential Regulation Authority (APRA)-regulated entities are required to comply with prudential standards on outsourcing and guidelines on outsourcing (CPS 231, SPS 231 and HPS 231) under which an APRA-regulated institution and the head of a group have ultimate responsibility for the outsourcing policy of the institution or group.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

APRA published an updated information paper in August 2018 on Outsourcing involving cloud computing services. In the information paper, APRA stated that it is prudent for an APRA-regulated entity to only enter into cloud computing arrangements where the risks were adequately understood and managed, by demonstrating:

- ability to continue operations and meet obligations following a loss of service or other disruption scenarios;
- preservation of the quality and security of critical and sensitive data;
- compliance with legislative and prudential requirements; and
- absence of other considerations that may inhibit APRA's ability to fulfil its duties as prudential regulator.

Financial services providers engaging cloud computing services should ensure that use of cloud computing complies with its obligations to protect personal information under the Privacy Act. This includes stipulating in contracts with cloud service providers that it will comply with the Australian Privacy Principles set out in the Privacy Act.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

The key intellectual property rights for protecting software include copyright, patents and trade secrets.

Copyright

New software in the form of code is protected as an original literary work under the Copyright Act 1968 (Cth). Copyright is automatically conferred over the software when it is created and does not require any form of registration under Australian law. Copyright provides the owner with an exclusive right to make copies of, publish, distribute and license the relevant works protected by copyright (such as the code for the software). Copyright does not protect the functionality of the software but the specific form of expression of the code or other relevant work. To protect the functionality of software, patent protection would often need to be considered.

Patents

Patents are a form of monopoly right that protect inventions, methods or processes that are sufficiently novel and inventive. A standard patent can provide protection over the patented invention, method or process for up to 20 years from the filing date. Obtaining a patent in Australia requires filing an application with IP Australia and prosecuting that application to registration. Applicants must be able to demonstrate that the relevant invention, method or process is sufficiently novel, inventive and otherwise meets the requirements for patent protection. Patents for software or components of software can be difficult to obtain under Australian law. In addition, use of the relevant software can impact on the validity of any subsequently filed patent application (meaning that advice regarding patentability of the software often needs to be sought as early as possible).

Trade secret

Aspects of the software could be protected as a trade secret, including under confidentiality obligations with employees, contractors and other third parties.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Ownership of IP developed by employees or contractors will generally be based on the terms stipulated in the relevant employment or consultancy contract.

In the event that the contract is silent on ownership rights (or no contract is in place), IP created by an employee in the course of the employment of the employee will generally be owned by the employer, whereas IP created by a contractor will generally remain the property of the contractor.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

A joint owner's right to deal with intellectual property (IP) depends on the type of IP and on the terms of any agreement in place between the owners.

The general rule for patents (unless an agreement says otherwise) is that joint owners are entitled to an equal undivided share in the patent and can exploit the patent for their own benefit without requiring consent from the other joint owners. However, a joint owner would not be able to grant a licence or assign an interest in the IP without the consent of the other joint owners.

In contrast, the general rule for copyright and trademarks (unless an agreement says otherwise) is that joint owners cannot exploit the relevant copyright or trademarks for their own benefit without the consent of the other co-owners and cannot licence or assign their interest in the IP without the consent of all other co-owners.

Joint ownership of IP is complex and frequently gives rise to disputes and uncertainty. As a result, caution should be exercised before agreeing to arrangements involving joint ownership of IP.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Trade secrets are not registered with IP offices (unlike many other forms of IP) and are protected by keeping the relevant information a secret and under contractual and equitable duties of confidentiality.

This can be effected by limiting access to confidential information and entering into non-disclosure agreements with employees, contractors and partners (which impose contractual restrictions on the use of the relevant trade secrets). Section 183 of the Corporations Act discourages officeholders and employees of a corporation from using or disclosing company information (such as trade secrets) for their own benefit or to the detriment of the company.

There can also be equitable duties of confidentiality that protect trade secrets, however, information in the public domain cannot generally be protected as confidential information.

Trade secrets may be kept confidential during court proceedings pursuant to suppression or other orders made by the court.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Branding is usually protected by trademark registration. A fintech business can apply for trademark registration through IP Australia. Registration involves nominating the trademark the business wishes to protect, selecting the goods and services that the trademark would be protected for and filing an application for trademark registration with IP Australia. The application would then need to be prosecuted through to registration.

In Australia, trademark registration lasts (once the mark is registered) for 10 years from its filing date. Fintech businesses can have trademark searches conducted to assess whether they are at risk of infringing existing brands. Copyright may also subsist in logos or other artwork used as part of the branding of a fintech business.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

Where IP rights have been infringed, the owners of IP are primarily responsible for enforcing their rights.

The first step for IP owners is often to send a letter of demand setting out the infringing conduct and requesting that the infringement be ceased. If the infringer is unresponsive to the letter of demand, the IP owner may seek recourse by alternative dispute resolution or court proceedings.

The exact remedies available will depend on the nature of the IP infringed and the jurisdiction and courts in which proceedings are commenced. However a court may have the power to award remedies such as:

- injunctive relief (interim and (or) final);
- damages or account of profits (including potential additional or penalty damages in certain circumstances, such as where an infringement is flagrant); or
- delivery up of infringing items.

A successful party may also be able to obtain an order for payment of its costs of the proceedings (although often this will not result in recovery of the full amount of costs actually incurred).

Registered IP rights are protected by (and available remedies depend on) different legislative schemes based on the type of IP, such as the Copyright Act 1968 (Cth), the Patents Act 1990 (Cth), the Trade Marks Act 1995 (Cth) and the Designs Act 2003 (Cth). In addition, other laws can be used to seek to protect the rights of an IP owner, for example, a common law claim for 'passing off' or claims for misleading and deceptive conduct or false or misleading representations under the Australian Consumer Law.

Read this article on Lexology

IP owners may also seek remedies for other relevant causes of action (namely, breach of confidence, breach of contract).

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

The consumer data right for the banking industry promises benefits of greater competition for existing financial services and more competitive pricing in the banking sector.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

While there are no tax incentives specific to fintech companies, there are a number of tax incentives encouraging innovation and investment generally, including for R&D, early stage innovation companies (ESIC), early stage venture capital limited partnerships (ESVCLP) and employee share schemes (ESS).

Tax incentive for companies: R&D

The R&D tax incentive encourages innovation through R&D activity. Eligible companies may receive an R&D tax offset if they have eligible R&D expenses of at least A$20,000. Eligible R&D expenses include expenditure incurred on R&D activities and depreciation on assets used for conducting R&D activities.

The quantum and nature of the R&D tax offset depends on the type of company:

- for small companies with less than A$20 million aggregated turnover and not controlled by exempt entities – a refundable tax offset of 43.5 per cent, or in limited cases 48.5 per cent (applied against notional R&D deductions) with no cap on cash refunds; and
- for all other companies – a non-refundable tax offset of between 33.5 per cent and 46.5 per cent (applied against notional R&D deductions) and any unused offset can be carried forward to later years.

Tax incentive for investors: ESIC

Investors that purchase new shares in a company that qualifies as an ESIC may be eligible for tax incentives including:

- non-refundable carry forward tax offset equal to 20 per cent of the amount paid for the shares. The tax offset is capped at a maximum amount of A$200,000 for the investor and their affiliates each income year (namely, a tax offset will apply to the first A$1 million of ESIC investments each year); and
- modified capital gains treatment under which capital gains on the ESIC shares that have been held for a period of between 12 months and 10 years may be disregarded.

For a company to be an ESIC, it cannot be a foreign company under the Corporations Act. It must prove that it is an early stage company and satisfy an innovation test. Even if the company ceases to be an ESIC at a later point in time, shares purchased by investors while the company was an ESIC continue to qualify for the tax incentives.

Tax incentive for investors and fund managers: ESVCLP

The ESVCLP programme is intended to help fund managers attract pooled capital to invest in early-stage businesses. An ESCVLP is a venture capital fund structured as a limited partnership or incorporated limited partnership that is established in Australia (or a country with which Australia has a double tax agreement) with between A$10 million and A$200 million in committed capital.

Investors in an ESVCLP benefit from the flow-through tax status of the partnership and are exempt from tax on their share of gains from eligible investments (or disposal of investments) as well as a non-refundable carry forward tax offset of up to 10 per cent of the value of their eligible contributions into the ESVCLP. Fund managers can claim their carried interest in the ESVCLP on capital account (which may be concessionally taxed) rather than revenue account.

Tax incentive for employees: ESS incentives

Fintech businesses may incentivise their staff by issuing equity (options or shares) under an employee incentive scheme. Ordinarily, the acquisition of discounted shares or options could be taxable upfront to employees. Where the employee shares or options qualify under the ESS rules, employees can defer their taxing point until exercise or, if the company qualifies as a 'start-up company' for tax purposes, tax can be deferred until disposal and only 50 per cent of the gain may be subject to tax.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

There are no new or proposed laws that would significantly increase tax for fintech companies.

Treasury released a discussion paper on October 2018 regarding digital services tax policies, however, in March 2019, the Treasurer announced that the government would not proceed with an interim digital services tax, but would instead engage in a multilateral process led by the OECD and G20.

The current tax treatment of digital assets results in a taxable event occurring on the disposal of digital assets. This can be onerous as it could result in a tax liability even where there is no cash gain (namely, where there is a crypto-to-crypto transaction). It can also be administratively burdensome as detailed tracking of asset movements is required to substantiate the amount of gain or loss. In its October 2021 report, the Senate Select Committee on Australia as a Technology and Financial Centre recommended that the capital gains tax regime be amended so that digital asset transactions only create a taxable event when they genuinely result in a clearly definable capital gain or loss. Draft legislation to give effect to this announcement has not been released at the date of this publication.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

A streamlined visa pathway is available for highly skilled professionals in target sectors including digitech, financial services and fintech through the Global Talent (subclass 858) visa. The Global Talent visa allows visa holders to stay in Australia permanently.

Employers can sponsor highly skilled staff under the Global Talent Employer Sponsored (GTES) scheme if the roles cannot be filled by Australian workers or through other standard visa programs. The roles for staff recruited under the GTES scheme are not limited to occupation lists. Instead, it is specific to the industry and if the person is working in the fintech sector, they qualify for the GTES option.

There is also the Global Talent Independent option, which requires the individual needs to prove they are capable of earning above the Fair Work High Income Threshold (currently A$162,000), have a distinction average academics and is seen as an industry leader with work regularly cited leading journals or publications.

Other avenues for fintech businesses to recruit skilled staff include:

- temporary skill shortage (subclass 482) visa, which generally allows visa holders to stay in Australia for up to four years if the worker has an occupation on the list of skilled occupations (which includes roles in technology and financial sectors); and
- employer nomination scheme (subclass 186) visa, which allows visa holders to stay in Australia permanently if the worker has an occupation on the list of skilled occupations.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

Traditionally, Australia has been a neutral jurisdiction in relation to blockchain and cryptocurrency regulations, however, recently, various regulatory bodies have addressed the digital assets space.

Cryptocurrency and other digital assets are currently being considered for various regulatory regimes relating to:

- licencing;
- marketing;
- cross-border issues;
- design and distribution obligations;
- Product intervention powers;
- consumer law; and
- taxation.

Further, in the buy now, pay later space, there will be further regulation that will ensure that service providers hold an Australian credit licence and comply with the relevant obligations.

Additional emerging trends to note include new payments platform with open access infrastructure, and digitisation, allowing instant payments .

There has been an increased interest in the use of blockchain technology in startups, established businesses and government agencies, with diverse use cases such as managing digital currency exchanges, issuing bonds, inter-government ledgers and authentication of trademarks. From a regulatory perspective, key focus points include:

- ensuring a robust regulatory framework in relation to crypto assets;
- developing policy options in relation to de-banking;
- addressing the increasing use of decentralised finance, non-fungible tokens and unhosted wallets in illegal financing activities; and
- a licensing and custody regime for crypto asset secondary services providers such as crypto exchanges and custody services.

John Bassilios john.bassilios@hallandwilcox.com.au

Level 11 Rialto South Tower, 525 Collins Street,
Melbourne VIC 3000, Australia
Tel: +61 3 9670 9632
www.hallandwilcox.com.au

Read more from this firm on Lexology

Read this article on Lexology

Belgium

Jérémie Doornaert, Martin Carlier, Ellen Herinckx and Raf Thielemans | Simmons & Simmons
Marc De Munter | Baker Tilly

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 29
General innovation climate 29
Government and regulatory support 30

FINANCIAL REGULATION 31
Regulatory bodies 31
Regulated activities 31
Consumer lending 33
Secondary market loan trading 33
Collective investment schemes 33
Alternative investment funds 34
Peer-to-peer and marketplace lending 34
Crowdfunding 34
Invoice trading 35
Payment services 36
Open banking 36
Robo-advice 36
Insurance products 37
Credit references 37

CROSS-BORDER REGULATION 38
Passporting 38
Requirement for a local presence 38

SALES AND MARKETING 38
Restrictions 38

CRYPTOASSETS AND TOKENS 40
Distributed ledger technology 40
Cryptoassets 41
Token issuance 42

ARTIFICIAL INTELLIGENCE 42
Artificial intelligence 42

CHANGE OF CONTROL 43
Notification and consent 43

FINANCIAL CRIME 43

Read this article on Lexology

Anti-bribery and anti-money laundering procedures 43
Guidance 44

DATA PROTECTION AND CYBERSECURITY 44
Data protection 44
Cybersecurity 46

OUTSOURCING AND CLOUD COMPUTING 47
Outsourcing 47
Cloud computing 47

INTELLECTUAL PROPERTY RIGHTS 48
IP protection for software 48
IP developed by employees and contractors 48
Joint ownership 49
Trade secrets 49
Branding 50
Remedies for infringement of IP 50

COMPETITION 51
Sector-specific issues 51

TAX 52
Incentives 52
Increased tax burden 53

IMMIGRATION 53
Sector-specific schemes 53

UPDATE AND TRENDS 54
Current developments 54

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

The Belgian fintech ecosystem continues to evolve and grow. In the early years of fintech and blockchain technology Belgian fintech companies were launched with a broad business idea, but the number of start-ups active in the financial sector with a more specific investment strategy in the technological sector has increased steadily. Further, whereas in the beginning fintech was reserved for established companies in the financial sector such as financial institutions and other financial actors, fintech is finding its way to nearly all sectors, through strategic partnerships to acquire new customers (a recent Belgian example is Banx, a mobile banking app offering more sustainable banking, launched as a result of a collaboration between Proximus, a telecom operator, and Belfius, a banking and insurance company). Fintech initiatives are set up through collaborations with start-ups, by using innovative technologies, such as distributed ledger technology (DLT), to evade the increasingly stringent regulatory environment in the financial sector.

Read this article on Lexology

More recently, fintech companies are looking for consolidation to create synergies and grow through acquisitions resulting in a surge of mergers and acquisitions activity in the fintech sector. For instance, the fintech fund Motive Partners recently acquired the investment fund Embedded Capital. In terms of fundraising fintech companies are attracting investments to enter new markets. The Belgian crypto service provider Keyrock raised US$72 million in a series-B financing round to expand their activities towards markets for non-fungible tokens, the blockchain market, over-the-counters and derivatives on digital assets.

However, Belgium is generally still lagging compared to other European countries, with Belgian fintech companies being unable to raise (venture) capital with the same ease as other European fintech companies such as Revolut (UK) or Mollies (the Netherlands). In effect, Belgian fintech companies tend to rely more on organic growth and to focus on underlying services for other companies, with less public attention as a result and taking more time to cross the Belgian border. Transforming all these promising start-ups into scale-ups capable of competing on the international scene is therefore a major challenge that requires stronger financial support and legislative reforms.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

No. However, the Belgian legislator introduced in the Omnibus Law of 27 June 2021, a legal framework for the use of new technologies for the holding and the settlement of securities, to allow central securities depositaries (CSDs) and account holders to keep their securities accounts in or through 'secured mechanisms for electronic registration'.

At the EU level, the pilot regime for market infrastructures based on distributed ledger technology (DLT) has been finalised (namely, the DLT Pilot Regime), offering a regulatory sandbox for eligible firms. The DLT Pilot Regime allows firms to test DLT-based trading facilities and settlement of digital securities (including tokenised financial instruments). Eligible firms can lodge their application with the national competent authority as from 23 March 2023. This should help EU regulators to overcome regulatory gaps in the existing regulation.

Further, Belgium has not implemented a sandbox. But both the National Bank of Belgium (NBB) and the Financial Services and Markets Authority (FSMA) offer fintech companies the opportunity to enter into direct contact with them through a dedicated fintech portal available on their websites. The purpose of the FSMA and NBB's FinTech Contact Point is to support a dialogue between the regulator and fintech companies, whereby the regulator aims to get back to the firms within three business days and to assist them in understanding the applicable regulatory framework. This facility can be used, for example, for guiding firms through the complex regulatory framework or any project relating to crowdfunding, distributed ledger technology, virtual currencies, application programming interfaces or alternative distribution models.

In addition, the merged platform, called startups.be | Scale-ups.eu, is a growth platform connecting promising start-ups and scale-ups with investors, global partners and high-tech companies.

Read this article on Lexology

Finally, a sectorial association called Fintech Belgium has been created, regrouping around 100 Belgian fintech companies.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

Based on the twin peaks model, both the Financial Services and Markets Authority (FSMA) and the National Bank of Belgium (NBB) are generally the supervisory authorities responsible for regulating the provision of fintech products and services in Belgium. Each regulator has a specific set of objectives. The NBB is the principal prudential supervisor for (among others) banks, insurance companies, stockbroking firms, payment and e-money institutions, on both a macro and micro level. The FSMA is responsible for supervising the financial markets and the information circulated by companies, certain categories of financial service providers (including investment firms and fund management companies) and intermediaries, compliance by financial institutions with conduct of business rules and the marketing of financial products to the public. The Federal Public Services Economy, small and medium-sized enterprises (SMEs), and Self-employed and Energy (FPS Economy) also have certain supervisory powers (eg, consumer credit, payment services).

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Fintech companies are not subject to a specific fintech licensing requirement. However, based on their structuring and activities deployed in Belgium, various licensing requirements can be triggered for a large number of financial activities. The following providers of financial services are regulated (among others):

- credit institutions;
- certain lenders;
- stockbroking and investment firms;
- fund management companies;
- virtual asset providers;
- payment institutions;
- e-money institutions; and
- insurance and reinsurance firms.

Only credit institutions may receive deposits from the public in Belgium or solicit the public in Belgium in view of receiving deposits. Credit institutions are regulated by the Belgian Act of 25 April 2014 relating to the status and supervision of credit institutions and stockbroking firms. Besides deposit-taking, the majority of the activities listed under Annex I of the Capital Requirements Directive may only be carried out by entities that are licensed or subject to specific regulations, or both. Certain lenders are also subject to local supervision (eg, consumer lenders and consumer mortgage lenders). Commercial lending (on a standalone basis) does not require a licence, but specific rules of conduct apply when lending to

SMEs. These rules of conduct include a duty of rigour, a duty of information and a right of prepayment for the enterprise. SMEs are individuals or legal entities pursuing an economic purpose in a sustainable manner or liberal professions (eg, lawyers and notaries) that have no more than one of the following criteria in their last and penultimate closed financial year:

- 50 employees on an annual basis;
- annual turnover of €9 million; and
- total balance sheet of €4.5 million.

All investment services contemplated by the second Markets in Financial Instruments Directive (MiFID II) are regulated and may only be carried out by duly licensed entities. Investment services include:

- reception and transmission of orders;
- execution of orders;
- proprietary trading;
- portfolio management;
- investment advice;
- underwriting and placing of financial instruments and operation of multilateral trading facilities, where they are carried out in respect of financial instruments such as transferable securities (shares, bonds, puts or calls on shares or bonds, etc);
- money market instruments;
- units in collective investment undertakings; and
- derivative contracts and instruments.

Dealing in foreign exchange spot and forward contracts (on one's own account or as an agent) is also regulated in Belgium. Investment services are carried out by (Belgian or foreign) investment firms. Belgian investment firms can be set up either as stockbroking firms (subject to the Act of 25 April 2014 relating to the status and supervision of credit institutions and stockbroking firms) and portfolio management and investment advice firms (subject to the Act of 25 October 2016 on investment firms and services).

Payment services institutions and e-money institutions are regulated by the Act of 11 March 2018, which implemented the second Payment Services Directive (PSD2) in Belgium. Insurance and reinsurance companies are ruled by the Act of 13 March 2016. Insurance contracts are regulated by the Act of 4 April 2014.

Intermediaries in banking and investment services, insurance intermediaries and consumer credit intermediaries are also subject to local supervision.

It is an offence to carry out any of the above-regulated financial services in Belgium without being duly licensed by or registered with the relevant regulator, subject to applicable EU passporting rules.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Consumer lending is a regulated activity in Belgium under Book VII of the Belgian Code of Economic Law. 'Consumer' means any individual acting for purposes that do not fall within his or her trade, business, craft or professional activity.

A licensing requirement applies to consumer lenders (including consumer mortgage lenders) and intermediaries in consumer lending. Certain (limited) exemptions are available. In addition, there are ongoing requirements that have to be complied with by the lenders (eg, provision of information, documents and statements, and form and content of the credit agreement itself).

Secondary market loan trading

6 | Are there restrictions on trading loans in the secondary market in your jurisdiction?

Provided that the borrowers do not qualify as consumers and the loan itself is being traded (and not a loan instrument), there are in principle no restrictions on trading (receivables in respect of) loans in the secondary market in Belgium. However, the loan agreement must not prohibit the assignment and civil law requirements may have to be complied with to ensure the enforceability of the transfer of the loan vis-à-vis third parties (and, as the case may be, the security rights attached thereto).

Receivables in respect of consumer loans may only be transferred to a limited number of assignees (including credit institutions, regulated lenders, credit insurers and a specific category of collective investment scheme designed for making investments in receivables, the *société d'investissement en créances* or *vennootschap voor belegging in schuldvorderingen*). The transfer of consumer mortgage loans is also subject to specific rules.

Collective investment schemes

7 | Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

In Belgium, collective investment schemes (CISs) and the management of CISs are regulated entities and activities respectively. In general, a CIS is any entity whose purpose is the collective investment of financial means collected from investors through an offer of financial instruments. The persons participating in the scheme (the investors) must not have day-to-day control over the management of the property. Further, the contributions of the participants and the profits or income out of which payments are to be made to them must be pooled and the property managed as a whole.

Whether a fintech company will fall within the scope of this regime will depend on the exact nature of its business. Fintech companies that manage assets on a pooled basis on behalf of investors should give particular consideration to whether they may be operating a CIS.

Read this article on Lexology

Fintech companies that are geared more towards providing advice or payment services may be less likely to operate a CIS, but should nonetheless check this and have regard to their other regulatory obligations.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

Managers of alternative investment funds are regulated in Belgium under the AIFMD, which was implemented in Belgium by the Act of 19 April 2014 relating to alternative investment funds and their managers, implementing royal decrees and circulars and guidance issued by the FSMA.

Peer-to-peer and marketplace lending

9 | Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

There are currently no (consumer) peer-to-peer lending platforms operating in Belgium. The Belgian regulatory framework does not currently authorise direct lending by consumers to consumers. The main legal obstacles are, first, the banking monopoly in Belgium relating to deposit-taking, and second, that the Belgian prospectus regulations prevent individuals from raising funds publicly, even with the intervention of a platform. In practice, this means that an individual cannot solicit the public to lend him or her money. Consumer lenders must be approved by the FSMA and only approved lenders have access to the Central Individual Credit Register (CICR).

However, alternative ways to structure this type of lending are possible, for example, by using an indirect lending model whereby a legal entity is interposed between the lenders and the borrowers. In such an indirect model, there is no direct relationship between the lenders and the borrowers. The legal entity must be approved by the FSMA as a (consumer) lender and grants the loans to the borrowers. To finance the loans, the legal entity issues notes, which typically replicate the repayment characteristics of the underlying loans and can be subscribed to by the lenders (in principle, based on a prospectus approved by the FSMA).

Peer-to-peer lending mainly differs from lending-based crowdfunding by the fact that the borrowers are individuals or consumers borrowing for private purposes.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

The Crowdfunding Regulation (accompanied by a Crowdfunding Directive) establishes a uniform framework for crowdfunding service providers and introduces an EU passporting regime, aimed at removing obstacles in the cross-border provision of crowdfunding services. The harmonised legal framework for crowdfunding service providers was implemented in Belgium by the Law of 23 February 2022, which amended the Belgian law on crowdfunding platforms of 18 December 2016 (the Belgian Crowdfunding Act) in relation to aspects not

addressed in the Crowdfunding Regulation. The FSMA published new FAQs on the conditions for authorisation and on the conduct of business rules for crowdfunding service providers.

The Crowdfunding Regulation is applicable to crowdfunding services, including both lending-based and equity-based crowdfunding services. Equity-based crowdfunding services are defined as a placing without a firm commitment basis of transferable securities and admitted instruments for crowdfunding purposes issued by project owners or a special purpose vehicle, and the reception and transmission of client orders. Crowdfunding services provided to project owners that are consumers or crowdfunding offers with a consideration of more than €5 million (calculated over a period of 12 months) do not fall within the scope of the Crowdfunding Regulation. Offers that exceed the threshold of €5 million need to issue a prospectus under the Prospectus Regulation, subject to approval by the FSMA, and might trigger the authorisation requirement under MiFID II. Only legal persons can provide crowdfunding services and are referred to as crowdfunding service providers (CFSPs).

Before providing any crowdfunding services in Belgium or on a cross-border basis, CFSPs must be authorised by the FSMA. Further, CFSPs must meet certain licensing requirements (incorporation and capital requirements) and are subject to rules of conduct (conflicts of interest, reporting and recording obligations, entry knowledge assessment and simulation of the ability to bear loss, etc). CFSPs shall provide prospective investors with a key investment information sheet drawn up by the project owner for each crowdfunding offer. The CFSP must ensure that the information sheet is correct, clear and complete.

Crowdfunding platforms are defined as publicly accessible internet-based information systems operated or managed by a crowdfunding service provider. Regulated companies are no longer exempted from the licensing requirement and need to request an authorisation if they want to continue providing crowdfunding services.

Marketing communications can be carried out to prospective investors or project owners about crowdfunding services provided by CFSPs in the same language as the key investment information sheet (being one of the official Belgian languages or in English).

Existing crowdfunding platforms, falling in the scope of the Crowdfunding Regulation, must apply for a licence under the new regime and can make use of a transitional period until 10 November 2022 at the latest to obtain an authorisation.

CFSPs duly licensed in Belgium benefit from EU passporting rights and can provide crowdfunding services in another member state of the European Economic Area on a cross-border basis without a permanent establishment or through a branch, provided that some information is shared with the FSMA (target member states, the identity of the responsible persons and scheduled starting date in these member states, as well as a list of other activities not covered by the Crowdfunding Regulation).

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

Factoring (on a stand-alone basis) is not a regulated activity. In Belgium, factoring is based on the transfer of ownership of the accounts receivable. It is the activity whereby the factor

(the buyer of the receivables) pays an agreed percentage of approved debts in exchange for the transfer of the related receivables by the client (the seller of the receivables).

A distinction is made between 'non-recourse' factoring (where credit protection is part of the factoring agreement) and 'with recourse' factoring (where the credit risk on the debtors of the receivables remains with the seller).

Some factoring contracts (also referred to as 'invoice discounting') permit the client to manage the receivables on the factor's behalf. The contract generally provides that this option can be switched off if the client does not comply with its obligations with due and proper care.

Payment services

12 Are payment services regulated in your jurisdiction?

Yes. Payment services are regulated by the Act of 11 March 2018, which implemented the PSD2 in Belgium. A firm that provides payment initiation services or account information services in or from Belgium as a regular occupation or business activity (and is not exempt) must apply for registration as a payment institution.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

Pursuant to the implementation of the PSD2 into Belgian law by the Act of 11 March 2018, financial institutions holding 'payment accounts' (eg, current accounts, credit card accounts, prepaid card accounts) will be required to allow, for free, access to their customers' account information to third-party payment service providers, subject to the consent of the customer. From a technical point of view, third-party payment service providers could get either direct access to the account or indirect access through a dedicated interface, such as an application programming interface.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

There is no specific regulation on robo-advice in Belgium. Consequently, whatever the mechanism underlying the robo-adviser's functioning, the services it provides will be considered as (semi-) automated investment services relating to financial instruments within the meaning of the Law of 25 October 2016. This investment service will be considered either as investment advice or portfolio management and companies using robo-advice on a professional basis will be subject to regulatory requirements applicable to investment firms providing the above-mentioned services.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Yes. Insurance intermediaries must be licensed by the FSMA before starting their activities as broker, agent or sub-agent. Intermediaries who only act as 'introducers' (namely, who only provide general information without interfering with the practical execution of insurance contracts or with the handling of claims) are not subject to licensing requirements.

Insurance intermediaries must prove to the FSMA that they have sufficient professional knowledge and adequate experience, and they have to comply with ongoing requirements.

Further, Belgian law has introduced MiFID-like conduct of business rules in the insurance sector, which include rules on suitability assessment and inducements.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

There are two credit information registers: the CICR and the Central Corporate Credit Register (CCCR), which are both operated by the NBB.

The CICR records information relating to all consumer credits and mortgage loans contracted by natural persons for private purposes as well as any payment defaults resulting from these loans. The sharing of credit data is an obligation for regulated financial institutions (including banks, firms specialising in consumer credit or mortgage loans and credit card issuers).

Further, regulated lenders have an obligation to consult the CICR in the process of assessing the borrower's creditworthiness. Credit data to be reported in the CICR include the debtor's or co-debtor's identification details, the characteristics of the credit contract and the details of the overdue debt.

The CCCR records information on credits granted to legal persons (enterprises) and natural persons (individuals) in connection with their business activity. Participation in the CCCR is mandatory for some financial institutions, including:

- credit institutions established in Belgium and licensed by the NBB (also branches incorporated under foreign law established in Belgium);
- finance-lease companies established in Belgium and licensed by the FPS Economy;
- factoring companies established in Belgium; and
- insurance companies established in Belgium and licensed for classes 14 (guarantee insurance) and 15 (credit insurance) by the NBB.

Participants have to report each month to the CCCR all information on any current contract (granted amounts) and non-repayments. Participants, debtors as well as other central credit offices abroad may consult the data recorded in the CCCR.

Read this article on Lexology

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

All financial services benefiting from European passporting rights may be provided by EEA firms licensed in their home country under one of the EU single market directives (eg, the Banking Consolidation Directive, the Capital Requirements Directive, Solvency II, the second Markets in Financial Instruments Directive (MiFID II), the Insurance Mediation Directive, the Insurance Distribution Directive, the Mortgage Credit Directive, the Undertakings for Collective Investments in Transferable Securities Directive, the Alternative Investment Fund Managers Directive, the Payment Services Directive or the E-Money Directive) either on a cross-border basis without a permanent establishment in Belgium or through a Belgian branch.

To exercise this right, the firm must first provide notice to its home regulator. The directive under which the EEA firm is seeking to exercise passporting rights will determine the conditions and processes that the firm has to follow.

Further, under certain conditions and limits, non-EEA firms may be authorised to provide investment services (as defined under MiFID II) either on a cross-border basis in Belgium or through a Belgian branch.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

The Belgian regulator only grants licences to companies established in Belgium. However, EEA fintech firms may exercise passporting rights to provide services in Belgium. Under certain conditions and limits, non-EEA firms may also be authorised to provide (MiFID) investment services on a cross-border basis in Belgium or through a Belgian branch.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Financial products (such as investment products, savings products and insurance products)

Marketing materials for financial products are governed by the Royal Decree dated 25 April 2014 on certain information obligations for the marketing of financial products to retail clients and Financial Services and Markets Authority (FSMA) guidance, which regulate the advertising of financial products where distributed to retail clients. 'Marketing materials'

means any communication designed specifically to promote the acquisition of the product, irrespective of the medium used or the method of dissemination.

The general requirements are that:

- the information included in the marketing materials shall not be misleading or incorrect;
- only information relevant to the Belgian market should be presented;
- it is recommended to translate the marketing materials into French or Dutch as there is a general requirement that the marketing materials must be understandable by a retail investor (also, technical terms should be avoided or, if it is impossible to avoid using technical terms, they should be explained in a way that is easily understandable for a retail client where these terms appear);
- the marketing materials should not emphasise the potential benefits of the product without also giving a fair, balanced and visible indication of the risks, limits or conditions applicable to the product;
- the marketing materials should not disguise, mitigate or conceal important items, mentions or warnings;
- the marketing materials should not highlight characteristics that are not relevant or that are of little relevance for a sound understanding of the nature and the risks of the product;
- the information conveyed in the marketing materials should be in line with the information in the prospectus or any other contractual or pre-contractual information; and
- any advertisement should be clearly recognisable as such.

Further, detailed guidance is provided by the FSMA for the marketing materials to comply with the non-misleading information principle. Detailed content requirements apply. The presentation of performance figures is also highly regulated.

Consumer credit

The Belgian Code of Economic Law contains provisions on advertising, (pre-contractual) information requirements, misleading and aggressive commercial practices and unfair contract terms.

All advertising setting out the interest rate or the costs of the credit must be drafted in a clear, summarised and explicit way, and contain specific legal information that must be illustrated by a representative example. Advertising must also include the warning: 'Be aware, borrowing money costs money'. Some advertising practices are also prohibited – for example, encouraging consumers to regroup their existing credits, emphasising the ease and speed by which credit can be obtained and such like.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

The EU mechanism for distributed ledger technology (DLT), the DLT Pilot Regime, allows operators of market infrastructure to test distributed ledger technology in trading facilities and settlement systems for tokenised financial instruments. Firms can apply to the DLT Pilot Regime as of 23 March 2023 and, if successful, will receive a permission for a period of up to six years. As part of their authorisation, firms may be granted exemptions from certain requirements under the Central Securities Depositories Regulation and the Markets in Financial Instruments Regulation. Those exemptions are critical and allow firms to experiment with DLT released from certain obligations in the existing EU market infrastructure regulation.

Several legal and regulatory issues need to be carefully considered relating to the clearing, settling and recording of payments, securities, derivatives or other financial transactions. The impact of various rules and regulations must be analysed and may be relevant in respect of digital transformation initiatives, such as the Central Securities Depositories Regulation, the Settlement Finality Directive, the European Market Infrastructure Regulation, the Markets in Financial Instruments Directive and so on. Outsourcing arrangements also need to be carefully reviewed where regulated firms outsource technological innovations to third parties.

Fintech companies can contact the Financial Services and Markets Authority (FSMA) or the National Bank of Belgium via their FinTech Contact Point through which they can raise questions relating to innovative technologies, like distributed ledger technology, and the application of financial legislation in this respect.

Data protection requirements and customer data protection also need detailed analysis because of the transparency of transactions, which is inherent to the blockchain technology, and the fact that once data is stored it cannot be altered (this could be an issue for compliance with the right for rectification or the right to be forgotten).

Given that the nodes on a blockchain can be located anywhere in the world, the determination of the data controller, applicable law and competent courts in the case of litigation and the drafting of appropriate contractual provisions (and possible additional security measures for transferring personal data outside of the European Economic Area following *Schrems II* case law) in that respect is also essential.

A particular point of attention relates to the status of the decentralised autonomous organisations that are used to execute smart contracts, recording activity on the blockchain.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

In 2022, the Belgian legislator enacted a new legislative framework for virtual assets service providers (VASPs), including two sets of legislation:

- the Act of 1 February 2022 amending the Act of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash to introduce provisions on the status and supervision of providers of exchange services between virtual currencies and legal currencies and providers of custodian wallet services (the VASP Act); and
- the Royal Decree of 8 February 2022 on the status and supervision of providers of services for the exchange between virtual currency and fiat currency and providers of custodian wallets (the VASP Royal Decree).

As from 1 May 2022, providers of exchange services between virtual currencies and fiat currencies and of custodian wallet providers established on the Belgian territory (namely, entities incorporated under Belgian law or EU entities with a Belgian branch, distributor or other form of lasting (electronic) infrastructure in Belgium – eg, automated teller machines) are required to register with the FSMA for anti-money laundering (AML) purposes.

In terms of scope:

- Services for the exchange between virtual currencies and fiat currencies refer to services that consist of purchase and selling transactions, with own capital, whereby virtual currencies are exchanged for fiat currencies or fiat currencies for virtual currencies.
- Custodian wallet services refer to services to secure cryptographic private keys on behalf of its clients to hold, store and transfer virtual currencies.
- Virtual currencies are defined as 'a digital representation of value that is not issued or guaranteed by a central bank or government, that is not necessarily linked to a legally established currency and that does not have the legal status of currency or money, but that is accepted by natural or legal persons as a medium of exchange and that can be transferred, stored and traded electronically'. Only virtual currencies with an exchange or payment function are envisaged by the VASP Act and the VASP Royal Decree. Virtual currencies with only a utilisation function, like 'utility tokens', or an investment function, like 'security tokens', do not fall within the scope of the VASP Act and the VASP Royal Decree.

The VASP Act and the VASP Royal Decree introduce a prohibition for EU and non-EU natural persons and non-EU entities to provide custodian wallets or virtual currency exchanges services in Belgium, subject to imprisonment (of one month to one year) or a criminal fine (of between €400 and €80,000), or both. EU VASPs are not subject to an AML registration with the FSMA and can provide virtual currency exchanges or custodian wallets services on a cross-border basis (provided that they are not established in Belgium, eg, through a branch, distributor or other types of infrastructure).

Read this article on Lexology

The FSMA has introduced a new regulation, as approved by the Royal Decree of 8 February 2023, that imposes restrictive conditions on the marketing of cryptoassets to consumers in Belgium as part of a regular business activity or on an occasional basis against remuneration. The FSMA regulation tightens the rules relating to the commercialisation of virtual currencies. Advertisements in relation to virtual currencies may not contain information that is misleading or inaccurate. All advertisements must include the following statement: 'Virtual currency, real risks. In crypto, only the risk is guaranteed.' In addition, any advertisement intended to be broadcasted as part of a mass campaign (namely, the dissemination of advertisements to at least 25,000 consumers) shall be notified to the FSMA at least 10 days before it is broadcasted. The regulation will apply to all advertisements as from 17 May 2023 and any advertisement that was disseminated prior to this date will have until 17 June 2023 to comply with the requirements set out in the FSMA regulation.

The EU Markets in Cryptoassets Regulation (MiCAR) was approved on 20 April 2023 and is expected to apply in 2024. The MiCAR introduces an EU-wide regulatory regime for the regulation of cryptoassets. It will have a significant impact on the crypto service providers and includes regimes for issuance, crypto services, market abuse and sustainability disclosures. The implementation and supervision will raise particular questions, particularly in light of the existing Belgian regulatory framework.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

The FSMA issued a communication on ICOs in Belgium on 13 November 2017, building on a communication by the European Securities and Markets Authority on the same subject and the same date. While no specific regulatory rules are in place for ICOs, depending on its structuring it might fall within the scope of more generic Belgian laws such as the law implementing the Prospectus Directive and the law on crowdfunding platforms.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

Currently, there is no specific regulation on artificial intelligence (AI) in Belgium.

At the EU level, negotiations have started to introduce the AI Act and AI Liability Directive addressing some concerns AI raises with regard to safety, security and fundamental rights protection.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Shareholders intending to hold (directly or indirectly) a qualifying holding in certain regulated companies must make a prior notification to, and be approved by, the Financial Services and Markets Authority or the National Bank of Belgium, as appropriate. A qualifying holding means any direct or indirect holding that represents 10 per cent or more of the capital or voting rights, makes it possible to exercise a significant influence over the management of the undertaking, or both. There are additional thresholds at 20, 30 and 50 per cent and companies may decide to insert specific thresholds in their articles of association. In addition, shareholders ceasing to hold a qualifying holding, or reducing their holding below 10, 20, 30 or 50 per cent, must also make a prior notification to the relevant Belgian regulator.

Finally, shareholders who have acquired a direct or indirect holding of 5 per cent or more (or have reduced their holding to below 5 per cent) of capital or voting rights must make a notification to the relevant Belgian regulator within 10 business days of the acquisition.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

The Act of 20 July 2020 transposed Directive (EU) 2018/843 (the Fifth Anti-Money Laundering Directive) (AMLD5).

The transposition of this Directive is done, inter alia, by making a number of amendments to the Act of 18 September 2017 on the prevention of money laundering and terrorist financing and on restricting the use of cash (the AML Act).

In accordance with AMLD5, two types of virtual currency service providers (namely, providers engaged primarily and professionally in exchange services between 'virtual currencies' and 'fiat currencies' on the one hand and, wallet providers offering custodian services of credentials necessary to access virtual currencies, on the other) are now also included in the list of subject entities. As a result, they will be subject to, among other things, KYC obligations as provided under the AML Act.

Moreover, the aforementioned service providers now also have a registration obligation with the FSMA. The registration requirement under the AML Act and the process thereunder will be clarified by royal decree. However, to date, no royal decree providing further guidance in relation to these registration requirements, or the process thereunder has been enacted yet.

Finally, specific customer due diligence and know-your-customer obligations apply to e-money products. Fintech companies, regardless of whether they are authorised, ought to have appropriate financial crime policies and procedures in place as a matter of good governance and proportionate risk management.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no anti-financial crime guidance specifically for fintech firms. The general rules and standards set out for regulated financial institutions apply, particularly the circulars issued by the Belgian regulators (the National Bank of Belgium and the Financial Services and Markets Authority). These documents are helpful for non-authorised fintech firms and may inform their own internal financial crime policies and procedures.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

There are no regulations specifically governing the processing and transfer of personal data relating to fintech products and services.

However, the processing and transfer of personal data relating to fintech products and services shall be governed by the General Data Protection Regulation (GDPR), which took effect on 25 May 2018. The GDPR was implemented in Belgium by the Law of 30 July 2018 relating to the Protection of Individuals regarding the Processing of Personal Data and came into force on 5 September 2018. The GDPR, however, remains the principal legislation governing the processing of personal data as only few provisions of the Belgian law concern private companies. The GDPR provides how data controllers (the natural person or legal person, which, alone or jointly with others, determines the purposes and means of the processing of personal data) may process the personal data of living individuals (data subjects). The GDPR requires that businesses may only process personal data where that processing is done in a lawful, fair and transparent manner. The Belgian law provides some specific provisions on the consent, the processing of health-related and judicial data, the processing for statistical purposes or scientific research, exceptions to data subjects' rights, etc.

The GDPR requires that any processing of personal data must be done pursuant to one of six lawful bases for processing. The most commonly used lawful basis for processing is to obtain the consent of the data subject to that processing – in relying on this lawful basis, the business must ensure that consent is freely given, specific, informed and unambiguous, and capable of being withdrawn as easily as it is given. Other lawful bases for processing data include where that processing is necessary for the business to perform a contract it has with the data subject, or where required to comply with a legal obligation.

Read this article on Lexology

The GDPR also provides a set of rights for the data subjects, including the right to information, the right to access their personal data, to correct their personal data should it be inaccurate, the right to oppose (upon request and free of charge) the processing of their personal data for marketing purposes, the right to withdraw one's consent and the right to data portability.

The GDPR also differs from the previous regime in that it places a significantly increased compliance burden on businesses, including, for example, mandatory requirements to notify regulators of data breaches, obligations to keep detailed records on processing and requirements for most entities to appoint a data protection officer.

The Belgian Data Protection Authority is the body that controls compliance with the GDPR and applicable Belgian law by businesses. Data subjects now have the right to lodge a complaint with the Belgian Data Protection Authority. Significant administrative sanctions (up to the greater of €20 million and 4 per cent of the worldwide turnover) can be imposed following a breach of the GDPR.

Recital 26 of the GDPR states that where data has been processed such that it is truly anonymised, the principles within the GDPR do not apply to the processing of that data. Businesses will have to determine what steps must be taken to ensure that personal data is indeed truly anonymised.

The Article 29 Working Party (an EU body comprising representatives from data protection regulators across the member states) released Opinion 05/2014 on Anonymisation Techniques (in the context of the previous EU data protection regime). This Opinion discusses the main anonymisation techniques used – randomisation and generalisation (including aggregation). The Opinion states that when assessing the robustness of an anonymisation technique, it is necessary to consider:

- if it is still possible to single out an individual;
- if it is still possible to link records relating to an individual; and
- if information can be inferred concerning an individual.

In relation to aggregation, the Opinion further states that aggregation techniques should aim to prevent a data subject from being singled out by grouping them with other data subjects. While aggregation will avoid the risk of singling out, it is necessary to be aware that links and inferences may still be possible with certain aggregation techniques.

The position on anonymisation taken from the Article 29 Working Party's Opinion is broadly unchanged in the GDPR. The GDPR itself also gives limited guidance on anonymisation in Recital 26, requiring data controllers to consider a number of factors in deciding if personal data has been truly anonymised, including the costs and time required to de-anonymise, the technology available at the time to attempt de-anonymisation, and further developments in technology.

Read this article on Lexology

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

Belgium has implemented Directive (EU) 2016/1148 on Network and Information Security (the NIS Directive) by way of the Belgian Law of 7 April 2019 (entered into force on 3 May 2019) establishing a framework for the security of network and information systems of general interest for public security. The Law applies to sectors of banking and financial market infrastructure and establishes, among others, security and notification requirements for operators of essential services and digital service providers. Many practical aspects provided for in the Law of 7 April 2019 are further elaborated on in a Belgian Royal Decree dated 12 July 2019.

Directive (EU) 2015/2366 (the Payment Services Directive) entered into force on 12 January 2016, setting out, among others, rules concerning strict security requirements for electronic payments and the protection of consumers' financial data, guaranteeing safe authentication and reducing the risk of fraud. Belgium implemented the provisions of the Payment Services Directive by way of the Belgian Law of 11 March 2018. Regarding cybersecurity, the Law of 11 March 2018 stipulates a security policy containing a number of obligations for payment service providers.

Further, Regulation (EU) No. 526/2013 is of importance in the fintech sector, as it establishes the European Union Agency for Network and Information Security (ENISA). ENISA provides recommendations on cybersecurity, supports policy development and its implementation, and collaborates with operational teams throughout Europe for the purpose of contributing to a high level of network and information security within the European Union.

Moreover, on 13 September 2017, the European Commission published the Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) No. 526/2013, and on information and communications technology (ICT) cybersecurity certification. The Proposal reinforces ENISA's role in the areas where the agency is already competent, and introduces new areas where support is needed, in particular the NIS Directive, the review of the EU Cybersecurity Strategy, the upcoming EU Cybersecurity Blueprint for cyber crisis cooperation and ICT security certification.

Additionally, on 17 May 2017, the European Parliament adopted Resolution 2016/2243 on fintech: the influence of technology on the future of the financial sector. This resolution further underlines that regulation on the provision of financial services infrastructure needs to provide appropriate incentive structures for providers to invest adequately in cybersecurity and emphasises the need for end-to-end security across the whole financial services value chain. This resolution is non-binding and has a purely advisory function.

Finally, in March 2018, the European Commission adopted an action plan on fintech, setting out a number of steps that the Commission intends to take, one of which is to increase cybersecurity and the integrity of the financial system. The action plan mentions the fact that the European Parliament has called on the Commission 'to make cybersecurity the number one priority in the fintech action plan'. It states that the transposition by member states of the NIS Directive is ongoing but that gaps may remain in EU financial sector legislation that

Read this article on Lexology

should be filled to improve the sector's resilience. Therefore, we can expect this field to evolve in the near future.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Regulated entities outsourcing operational tasks of critical importance must ensure the continuous and satisfactory provision of services and activities. In this respect, they generally have to take appropriate measures to limit the associated operational risk. In particular, the outsourcing must not substantially affect the effectiveness of the internal control procedures of the company or the ability of the regulator to check whether the company is fulfilling its legal obligations. Prior notification and regulatory approval may be necessary.

The Financial Services and Markets Authority (FSMA) and the National Bank of Belgium (NBB) have both issued guidance or circulars on outsourcing by entities falling within their scope of regulatory powers.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

There are no specific legal requirements with respect to the use of cloud computing in the financial services industry. However, the outsourcing of cloud computing by regulated entities is subject to regulatory supervision from both a data protection and an IT security perspective.

Moreover, there are several requirements and guidelines that financial institutions in Belgium should be aware of when moving business functions to the cloud, including but not limited to:

- Circular NBB 2020-18 of 5 May 2020 on the recommendations of the Bank on outsourcing to cloud service providers, and the broadly equivalent provisions of the FSMA Circular 05-06.2007 on organisational requirements for firms providing investment services;
- Circular NBB 2009-17, financial services via the internet: prudential requirements, examines outsourcing risks and sets out the requirements for internal control and management of those risks. It also discusses compliance with the financial rules of conduct and the potential impact of cross-border transactions in the cloud; and
- Circular NBB 2015-32: additional prudential expectations regarding operational business continuity, and security of systemically important financial institutions, sets out management and security processes for institutions that play a critical role in the financial system, and whose disruption could jeopardise its proper functioning.

Read this article on Lexology

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Under Belgian law, computer programs (or software) are protected by copyright (article XI.294-XI.304 of the Belgian Code of Economic Law) and assimilated as literary works in the meaning of the Berne Convention. Copyright protection also covers the source code, object code, architecture of the software and preparatory design materials (provided that they can lead to a computer program). Ideas and principles that underlie any element of a computer program, including those that underlie its interfaces, are, however, excluded from the copyright protection.

The author of the software owns the rights as soon as it is created, provided that the software is original. No registration is required to benefit from the protection. For evidentiary purposes, it is, however, useful to include the name of the author and the creation date in the code of the software and to file it with a public notary or the Benelux Office for Intellectual Property.

If the software code has been kept confidential it may also be protected as confidential information. No registration is required, but confidentiality agreements are recommended if third parties have access to it.

Computer programs and business methods are explicitly excluded from patent protection. The exclusion from patentability is, however, limited to the software as such and it is possible to grant a patent to an invention implemented by or including a piece of software.

In Belgium, databases underlying software programs may also be protected by copyright (article XI.186-XI.188 of the Belgian Code of Economic Law) and, in certain circumstances, by sui generis database right (Book XI, Title 7 of the Belgian Code of Economic Law). The database right is a stand-alone right that protects databases that have involved a substantial investment in obtaining, verifying or presenting their contents (article XI.306 of the Belgian Code of Economic Law). Both database copyright and database rights arise automatically without any need for registration. Database rights do not apply to computer programs as such, including those used in the manufacture or operation of databases.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Unless otherwise provided in writing, where a computer program is created by an employee in the execution of his or her duties or following the instructions given by his or her employer, the employer will be exclusively entitled to exercise all economic rights in the computer program so created. This means that the IP rights subsisting in a computer program are automatically transferred to the employer when an employee has developed the software

in the framework of his or her employment contract. This automatic transfer only applies to the economic rights, not the moral rights of the author. The rule is different for other forms of IP rights, meaning that (except for the above-mentioned computer programs), IP that is created by an employee in the execution of his or her employment contract in principle belongs to the employee himself or herself, unless a clause explicitly stipulates that it belongs to the employer.

Where IP is developed by a contractor or a consultant, the rights are owned by the author of the software (namely, the contractor or the consultant). The fintech company will only own the economic rights if they have been explicitly transferred in writing (even if the fintech company has commissioned the software). The same goes for other IPs developed by a contractor or consultant. Therefore, contracts must be carefully drafted.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

There are no legal restrictions to the exercise of IP rights by a joint owner. However, in general, an agreement is required between the joint owners regarding their respective IP rights, in the absence of which the IP rights must be exercised jointly. There are certain exceptions to this, depending on the type of IP.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Belgium mainly implemented Directive (EU) 2016/943 (the Trade Secrets Directive) in Book XI of the Code of Economic Law. The Directive requires member states to provide protection for information that:

- is secret, in the sense that it is not generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question;
- has commercial value because it is secret; and
- has been subject to reasonable steps by the holder of the information to keep it secret.

If a competitor legally obtains the trade secrets or confidential information of a company, it is, in principle, free to use it. Therefore, it is highly recommended to be prudent regarding the persons to whom one discloses confidential information and to enter into proper confidentiality agreements with those persons. These confidentiality agreements should include provisions such as the definition of confidential information, the duration of the confidentiality obligations (knowing that under general Belgian civil law, it is always possible to terminate an obligation for an indefinite term against 'reasonable' notice, meaning that a fixed term should be provided in the confidentiality agreement) and the limited use of trade secrets and confidential information regarding the purpose of a specific project.

Legal proceedings are, in principle, public, so it would be possible to hear trade secrets and confidential information during hearings or pleadings. In addition, the Belgian Judicial

Code does not restrict access to documents including trade secrets – it provides for principles of collaboration as regards the production of evidence in court proceedings and the requirement for any party to submit all documents to the other party, without specifications or exceptions concerning trade secrets. In practice, however, it appears that, depending on the interest that is considered most relevant, Belgian (commercial) courts may choose to limit the production of evidence to certain elements or even block access to or disclosure of trade secrets (eg, if there is no sufficient evidence of a breach).

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brands can be protected by a Benelux trademark (covering the Benelux territory) or by an EU trademark (covering the EU territory). Registration is required to obtain a trademark right (with the Benelux Office for Intellectual Property for Benelux trademarks or with the European Union Intellectual Property Office (EUIPO) for EU trademarks).

Brands can also be protected by market practices if they have acquired sufficient goodwill in the market and another undertaking tries to take advantage of the reputation or market position of the brand.

Brands in the form of logos or slogans can also be protected by copyright as artistic works (provided they are original) or by Benelux or EU design and models rights (provided that they are new and have specific character).

The Benelux Office for Intellectual Property and EUIPO have public databases that can be consulted to check the availability of a design or trademark. It is highly advisable for new businesses to conduct trademark and design searches to check whether earlier registrations exist that are identical or similar to their proposed brand names. It may also be advisable to conduct searches for any unregistered trademark rights that have gained sufficient distinctiveness on the market that may prevent use of the proposed mark. Specialised companies offer services to carry out these searches.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

The following remedies and proceedings may be available:

- (unilateral) primary injunction;
- seizure-description;
- cease-and-desist action;
- damages; and
- application with customs authorities for border detention.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

Competition law (namely, Book IV of the Belgian Code of Economic Law and the EU competition rules in the case of an effect on trade between EU member states) applies to all undertakings carrying out business in Belgium, irrespective of their sector. Hence, the competition law rules (such as the prohibition of anticompetitive agreements, the prohibition of abuse of dominance, merger control and, in Belgium, abuse of economic dependence) apply to fintech companies.

While fintech is generally considered to be beneficial for consumers (because of cost reduction, improvements in efficiency, greater transparency and increased financial inclusion), it could raise competition law issues. Competition authorities in all jurisdictions, including Belgium, face a range of potentially complex competition law issues in relation to fintech offerings. These are likely to include:

- the extent to which a fintech solution has or obtains (through growth, acquisition or joint venture) market power (eg, because of big data or network effects) and the consequences of this;
- the extent to which the entrance of big tech into fintech will result in those companies tipping fintech markets into a situation of market dominance (eg, as a result of self-preferencing their respective ecosystems);
- the risks that the definition of any technical standards involved in any jointly developed fintech solution result in other third parties being excluded;
- whether banks are limiting access of fintech companies to bank accounts and thereby hindering competition in the payment market. The European Commission, in this context, conducted dawn raids in 2017 at the premises of banking associations in, among others, the Netherlands and Poland (the investigation is ongoing as at the time of writing);
- the extent to which there can be any exclusivity between the finance and technology providers of a fintech offering; and
- the limits of any specified tying or bundling.

On 9 July 2018, the Economic Affairs Committee of the European Parliament published a study regarding competition issues in fintech. The study concludes that the pro-competitive effects of fintech need to be weighed against the anticompetitive effects and that, currently, it would be better to research, monitor and regulate than to enforce through the usual competition tools (namely, investigate and sanction).

Just like the European Commission, the Belgian Competition Authority considers the digital sector as one of its enforcement priorities. Reference should in this respect be made to the European Commission's Digital Markets Act which, once adopted (expected in October 2022), will create various obligations and prohibitions for certain digital services companies of a certain size (gatekeepers).

The Belgian Competition Authority is likely to follow the enforcement policy of other EU member states in the field of fintech. Reference can in this respect in particular be made to the ACM (Dutch competition authority) and FCA (French competition authority), having conducted market studies regarding the role of big tech in fintech.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

In support of the Digital Belgium action plan, the Belgian federal government has introduced a number of tax incentives that are available to fintech companies and investors subject to certain conditions being met. These incentives include, among others:

- The Belgian tax shelter regime for start-ups, which provides for a tax reduction for physical persons who invest in start-ups, has been extended to direct and indirect equity investments via approved crowdfunding platforms. The tax reduction amounts to up to 30 per cent or 45 per cent of the invested amount (45 per cent in the case of a direct investment (possibly via a crowdfunding platform) in a micro-enterprise). The investment (shares) must be retained for at least four years to benefit from the tax shelter. Since assessment year 2019, the tax shelter system has been extended to new equity investments in growth companies, via capital increases in cash in the fifth to tenth year after their incorporation. The tax reduction amounts to 25 per cent of the investment.
- The provision of loans by physical persons via approved crowdfunding platforms is encouraged fiscally by a (withholding) tax exemption on the interest of the loans up to the first bracket of €15,630 (assessment year 2023) and this is for the first four years of the loan. This (withholding) tax exemption is subject to the loans having a minimum maturity of four years and is only applicable if the loans have been provided to start-up companies not older than four years.
- Start-up companies can benefit from reduced labour costs, via a retention of 10 per cent or 20 per cent (if the employer is a micro-enterprise) of the payroll tax withheld by the employer on the employee salaries.
- The new innovation tax deduction of 85 per cent of the net income realised by companies also applies to income and gains from copyright-protected software, including adaptations of existing software and derivative works.
- An increased deduction for investment in certain digital assets and environmentally friendly R&D investments and patents of 13.5 per cent of the acquisition value.
- Private individuals trading in bitcoins are not necessarily taxed on the gains as professional income, but insofar as the trade is speculative in nature (short holding period, high risk, etc), the gains may be taxed as miscellaneous income at 33 per cent, with an exemption from social security contributions.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

As far as we know, Belgium is not intending to launch a separate digital tax that could affect fintech companies, but closely monitors the Organisation for Economic Co-operation and Development's work on the digitalised economy. In particular, the current focus is on the OECD/G20 Inclusive Framework (Pillar One on revised nexus and profit allocation rules and Pillar Two on the development of a global anti-base erosion proposal and minimum tax proposal) to address the tax challenges arising from the digitalisation of the economy and what the impact (if any, taking into account the proposed exclusion of at least regulated financial services from Pillar One) may be of these proposals on, inter alia, the Belgian fintech sector. However, it cannot be excluded that a digital tax will be introduced in the future in the framework of tax reform, shifting taxation from labour to other types of income and profits.

The Belgian government is, however, intending to implement Pillar Two by the end of 2023. Moreover, the attractive personal income tax regime for royalties would in principle no longer apply to income from software development.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

To work in Belgium for longer than 90 days, foreign workers must have a valid work permit. This condition does not apply to nationals of an EEA member state (the countries of the European Union and Iceland, Norway and Liechtenstein) and Switzerland and to some categories of workers who are exempted.

Belgian employers must apply for a single permit if they want to employ a non-EEA worker.

Following the transposition of the EU Directive on intra-corporate transferees, new types of residence permits have been created in Belgium for employees who have at least a higher-education degree and who are employed before and during the temporary transfer, to an entity belonging to the company of the employer or to the same group of companies established in that EU member state.

There are no special regimes specific to the fintech sector.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

The evolving fintech landscape offers a wide range of innovative solutions and capabilities. However, new challenges impact the activities of fintech companies, like cyber threats and information security risks. The Financial Services and Markets Authority will continue to monitor these challenges and the FinTech Contact Point will be a useful tool to that end.

For virtual asset service providers established in Belgium, the entry into force of the VASP Act and the VASP Royal Decree as from 1 May 2022 introduced a significant change in the regulatory landscape of cryptocurrencies and will definitely play an important role in the near future.

simmons + simmons

Jérémie Doornaert	jeremie.doornaert@simmons-simmons.com
Martin Carlier	martin.carlier@simmons-simmons.com
Ellen Herinckx	ellen.herinckx@simmons-simmons.com
Raf Thielemans	raf.thielemans@simmons-simmons.com

Avenue Louise 143, Brussels 1050, Belgium
Tel: +32 2 542 09 60
www.simmons-simmons.com

Read more from this firm on Lexology

Baker Tilly

Marc De Munter	m.demunter@bakertilly.be

Inter Access Park, Pontbeekstraat
4 - B-1702 Groot-Bijgaarden, Brussels, Belgium
Tel: +32 2 229 32 60
www.bakertilly.be

Read more from this firm on Lexology

Read this article on Lexology

Bulgaria

Damian Simeonov, Nikolay Zisov, Svetlina Kortenska, Georgi Drenski and Stela Sabeva*

Boyanov & Co

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 56

General innovation climate 56
Government and regulatory support 57

FINANCIAL REGULATION 57

Regulatory bodies 57
Regulated activities 57
Consumer lending 58
Secondary market loan trading 59
Collective investment schemes 59
Alternative investment funds 60
Peer-to-peer and marketplace lending 60
Crowdfunding 60
Invoice trading 61
Payment services 61
Open banking 62
Robo-advice 62
Insurance products 62
Credit references 63

CROSS-BORDER REGULATION 63

Passporting 63
Requirement for a local presence 64

SALES AND MARKETING 64

Restrictions 64

CRYPTOASSETS AND TOKENS 64

Distributed ledger technology 64
Cryptoassets 65
Token issuance 66

ARTIFICIAL INTELLIGENCE 66

Artificial intelligence 66

CHANGE OF CONTROL 66

Notification and consent 66

FINANCIAL CRIME 67

Read this article on Lexology

Anti-bribery and anti-money laundering procedures 67
Guidance 68

DATA PROTECTION AND CYBERSECURITY 68
Data protection 68
Cybersecurity 71

OUTSOURCING AND CLOUD COMPUTING 71
Outsourcing 71
Cloud computing 72

INTELLECTUAL PROPERTY RIGHTS 72
IP protection for software 72
IP developed by employees and contractors 73
Joint ownership 73
Trade secrets 74
Branding 75
Remedies for infringement of IP 75

COMPETITION 76
Sector-specific issues 76

TAX 76
Incentives 76
Increased tax burden 77

IMMIGRATION 77
Sector-specific schemes 77

UPDATE AND TRENDS 78
Current developments 78

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

According to recent statistics reported by the Bulgarian Fintech Association, in 2022 there were 156 fintech companies in the country, most of them being small and medium-sized enterprises. In addition to these companies, most of the traditional financial institutions have made significant progress in digitalisation of their financial services. Currently, most of the Bulgarian banks offer advanced digital solutions, including mobile banking applications, digital customer loans and instant digital payments (eg, ApplePay). Some telecom operators also provide digital wallets and the ability to make payments through them. According to recent industry analysis, the largest contributor to the peak performance in the sector seems to be the digital payments segment, followed by enterprise technology provisioning companies, which enable application programming interface, management, cloud computing, artificial intelligence, machine learning and natural language processing, etc.

Read this article on Lexology

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

The Bulgarian government supports the fintech industry in various ways.

The competent regulator, the Financial Supervision Commission, is increasingly active in the sector. It adopted a strategy for monitoring financial innovation for the period 2021–2024. The strategy outlines the main approaches of action – monitoring of fintech development, assessing possible risks for the market and the consumers, and potential actions and measures to minimise them to maximise the benefits of growing interest in innovative financial products or technologies in compliance with regulatory requirements. InvestBulgaria, the Bulgarian investment promotions agency, provides active assistance and governmental support to foreign investors in the fintech sector. The agency aims to facilitate potential and existing direct investors with the implementation and establishment of their investment projects in Bulgaria through the provision of individualised administrative services and the implementation of various incentive measures.

Last, the Bulgarian government and private universities in Bulgaria encourage and develop various educational initiatives and programmes in the fintech sector. In February 2021, the Council of Ministers adopted the National Financial Literacy Strategy and respective Action Plan 2021–2025. The Action Plan provides specific measures aimed at developing educational content for digital financial services and products.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

The Bulgarian National Bank (being the national central bank, as well as the banking regulator) regulates the activities of credit institutions (banks), non-banking financial institutions, e-money institutions and providers of payment services. The activity of investment firms is regulated by the Financial Supervision Commission.

Regulated activities

4 Which activities trigger a licensing requirement in your jurisdiction?

Pursuant to article 2 of the Credit Institutions Act, receiving deposits or other repayable funds from the public, as well as acceptance of valuables on deposit and acting as a depository or trustee institution within the territory of the Republic of Bulgaria, may be carried out only by a bank licensed by the Bulgarian National Bank, a bank that has been granted a banking licence by the competent bodies of a European Economic Area (EEA) member state or a bank from a third country, which has been granted a licence by the Bulgarian National Bank to conduct banking business in Bulgaria through a branch. 'Receiving deposits or other repayable funds from the public' means receiving deposits or other repayable funds from

more than 30 persons who are not banks or other institutional investors. Where bonds or other debt securities are issued under terms and procedures other than the Public Offering of Securities Act, receiving deposits or other repayable funds from the public exists where:

- bond issues or other debt securities issues have been acquired at an initial offering by more than 30 persons who are not banks or other institutional investors;
- this is one of the principal activities of the issuer; and
- the issuer grants credits by the nature of trade thereof or provides other financial services by the nature of trade thereof.

Pursuant to the Credit Institutions Act, only a financial institution established and registered in Bulgaria and entered into a register maintained by the Bulgarian National Bank or a financial institution having its registered office in an EEA member state that has passported its activity in Bulgaria, may perform the following activities on the territory of Bulgaria as business and if this activity represents an essential part of its overall activity:

- financial leasing;
- guarantee transactions;
- acquisition of loan receivable and other types of financing (factoring, forfeiting, etc);
- acquiring shareholdings; and
- granting loans with funds that have not been raised from receiving deposits or other repayable funds from the public.

The requirements for such registration and the criteria to determine 'essential activity' are set out in an ordinance issued by the Bulgarian National Bank.

The provision of investment services requires an investment intermediary's licence issued or 'passported' for Bulgaria in accordance with the Bulgarian Markets in Financial Instruments Act, which transposes Markets in Financial Instruments Directive II (MiFID II). Bulgaria is an EU member state thus applying directly the Markets in Financial Instruments Regulation and related EU regulations with respect to requirements on undertaking investment services activities.

To sum up, investment services may be provided either by credit institutions licensed or passported to provide investment services or by investment intermediaries licensed or passported to provide investment services. While the Bulgarian National Bank is the primary regulator for credit institutions acting in cooperation with the Financial Supervision Commission so far as MiFID II activities are concerned, the Financial Supervision Commission is the exclusive regulator for investment intermediaries.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Lending to consumers may be provided as a business only by banks licensed by the Bulgarian National Bank or passported for the territory of Bulgaria or by financial institutions registered in the register of financial institutions maintained by the Bulgarian National Bank or operating from their seat outside Bulgaria on an unsolicited cross-border basis.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

Banks are allowed to purchase loan receivables provided that this activity is a part of their licence. A non-banking entity can perform such activity on the territory of Bulgaria, if such activity represents an essential part of its overall activity, only after it has been registered as a financial institution by the Bulgarian National Bank or has passported its activity for Bulgaria. Lending activity is deemed 'essential' when it represents not less than 30 per cent of the overall activity of the entity pursuant to its financial statements.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Collective investment schemes (CIS) in Bulgaria are regulated by the Collective Investment Schemes and Other Undertakings for Collective Investments Act (CISOUCIA).

The activities of CISs and other collective undertakings, as well as of the CIS managers and terms of conduct of their business, are regulated by the Financial Supervision Commission (FSC), Investment Activity Supervision Department, and respectively by the Deputy Chairperson of the FSC in charge of Investment Activity Supervision. A licence for pursuit of business as a CIS or for common fund organisation and management is granted by the FSC.

The Bulgarian CISOUCIA (as in other EU jurisdictions) adopts a holistic approach to all CIS (including regulation of alternative investment funds, undertakings for collective investments in transferable securities and exchange-traded funds). It also outlines the rules on regulatory authorisation of the administration, marketing and compliance with investment rules. In principle, management and distribution of CISs (namely, marketing, promotion and advertising) may only be carried out by licensed or authorised entities.

The FSC applies in its supervisory practice the recommendations and guidelines of the European Securities and Markets Authority and of the European Banking Authority in accordance with article 13, paragraph 1, item 26 of the Financial Supervision Commission Act.

Crowdfunding is subject to Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 (Crowdfunding Regulation). The application of the EU Crowdfunding Regulation is effective since the end of 2021 and its national application is secured by specific references in the Bulgarian Public Offering of Securities Act.

Whether a fintech company falls within the scope of this regulatory regime will depend on the exact nature of its business and the type of activities being carried out. The regulatory assessment shall be made in each particular case of companies providing alternative finance products, including peer-to-peer lending or crowdfunding platforms.

Read this article on Lexology

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Bulgaria is an EU member state and applies the Alternative Investment Fund Managers Directive 2011/61/EU as transposed in the CISOUCIA. Hence, a licence is required for alternative investment fund managers if they manage directly or indirectly alternative investment funds, the value of whose assets, as determined under Commission Delegated Regulation (EU) No. 231/2013 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositaries, leverage, transparency and supervision (OJ L 83/1 of 22 March 2013) in the aggregate exceeds:

- the Bulgarian leva equivalent of €100 million, including assets acquired using leverage; and
- the Bulgarian leva equivalent of €500 million, where portfolios consist of alternative investment funds not making use of leverage, and for which the right of redemption may not be exercised for a period of five years from the date of the initial investment in each of these alternative investment funds.

An EU management company will be able to undertake activity in Bulgaria either under the right to establishment or under the freedom to provide services following the conduct of the respective EU passporting procedure as set out in the CISOUCIA by notification made via its home regulator to the FSC.

An alternative fund manager requires registration in the FSC if it meets the regulatory qualification requirements that are set out in the CISOUCIA.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Bulgarian law does not regulate specifically peer-to-peer lending. If such activity is performed on the territory of Bulgaria the general regulatory regime of lending applies unless it is considered crowdfunding where the respective EU crowdfunding regulatory regime would be applicable.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business is in force and applies directly in Bulgaria. Bulgarian legislation provides that the competent authority under the Regulation, including for licensing, shall be the Financial Supervision Commission or, with respect to the banks, the Bulgarian National Bank.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

The regulatory regime of invoice trading follows the general regime of factoring.

Factoring services can be performed as a business by a licensed bank (if a part of its licence) or by a financial institution entered into a register maintained by the Bulgarian National Bank, or by a financial institution having its registered office in an EEA member state that has passported its activity in Bulgaria.

Pursuant to Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (Rome I), the law governing the assigned receivable, shall determine, inter alia, its assignability, the relationship between the assignee and the debtor, the conditions under which the assignment or subrogation can be invoked against the debtor and whether the debtor's obligations have been discharged. As a matter of Bulgarian law, receivables are generally transferrable by way of assignment unless the law, the nature of the receivables or the contract do not permit it.

In general, assignment of invoice receivables is not restricted by law or the nature of the receivables but the underlying agreement may prohibit such assignment.

Pursuant to the Consumer Credit Act and the Consumer Credits Related to Immovable Property Act, a creditor may assign its receivables under a consumer loan agreement to a third party only where the consumer loan agreement provides for such a possibility.

Payment services

12 | Are payment services regulated in your jurisdiction?

Payment services are regulated in the Bulgarian Payment Services and Payment Systems Act (PSPSA), which transposes the EU Payment Services Directive (PSD2). Subject to PSD2 exemptions as set out in article 2 of the Bulgarian PSPSA, an entity intending to provide payment services will need to obtain a licence as a payment services provider from the Bulgarian National Bank.

Under the PSPSA, payment services providers are:

- banks within the meaning of the Credit Institutions Act;
- electronic money institutions within the meaning of the PSPSA;
- payment institutions within the meaning of the PSPSA; and
- the European Central Bank and the national central banks of the EU member states when they do not act as monetary policy authorities or bodies performing public authority functions.

EU payment service providers may provide payment services in Bulgaria under the right to establishment or under the freedom to provide services following the conduct of the EU passporting procedure by notifying the Bulgarian National Bank via its home regulator in accordance with the provisions of the PSPSA transposing the respective provisions of PSD2.

Read this article on Lexology

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

No, there are no such specific laws or regulations although with the transposition of PSD2 in the PSPSA and the regulation of the payment initiation services, and the account information services as payment services, the basic framework for introducing open banking standards (including via application programming interfaces or otherwise) are generally in place.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

There are no specific regulations for robo-advisers or other companies that provide retail customers with automated access to investment products. Automated access to investment products through fintech companies in Bulgaria is only possible if the FSC has issued respective investment services licences.

Fintech companies may provide automated activities related to investment advice (when referring to specific financial instruments after taking into account the personal circumstance of the investor) and portfolio management, but these activities trigger investment intermediary licensing requirements and compliance with the applicable market standards and regulations under MiFID II, MiFIR and the related secondary acts.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Selling or marketing insurance products in Bulgaria is a regulated activity and entities providing such service fall under the relevant Bulgarian insurance regulations (which transpose the rules of Directive (EU) 2016/97 (Insurance Distribution Directive)). In this regard, a fintech company may sell or market insurance products under the form of a regulated entity – either as an insurance company, an insurance intermediary (broker or agent) or an ancillary insurance intermediary. The competent regulatory and supervisory body is the Financial Supervision Commission (and its deputy chair in charge for Insurance Supervision), which is empowered to issue licences to insurance companies (or acknowledge the passportisation in Bulgaria of such licences issued in other EU member countries) and to maintain a register of local insurance intermediaries (or acknowledge the passportisation in Bulgaria of similar licences or registrations issued in other EU member countries).

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Regulation (EU) No. 462/2013 of the European Parliament and of the Council of 21 May 2013 amending Regulation (EC) No. 1060/2009 on credit rating agencies applies directly in Bulgaria.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

EU-regulated entities licensed by their EU home regulators are entitled to provide services in Bulgaria under the EU right to establishment or under the EU freedom to provide services in Bulgaria following completion of the respective regulated industry's European Economic Area (EEA) passporting procedures for Bulgaria.

The EEA passporting procedure requires notification to be made via the competent home regulatory authority to the respective competent Bulgarian regulators. The notified Bulgarian regulators, namely – the Financial Supervision Commission for insurance, investment services and fund management services, or the Bulgarian National Bank – for credit institutions, payment institutions or e-money institutions, shall recognise the authorisation given to the EU regulated entity by its home regulator and shall notify the companies providing services in Bulgaria of any rules of public order or general good (for insurance businesses) to which these have to adhere when operating in Bulgaria and providing regulated services to Bulgarian customers on a cross-border basis.

EU financial institutions (other than credit institutions, payment institutions, e-money institutions, insurance companies or brokers or investment intermediaries) that are subsidiaries of credit institutions can also benefit from an alleviated regulatory authorisation to provide lending, financial leasing, factoring and forfeiting services. These shall be registered in the register of financial institutions of the Bulgarian National Bank on the basis of a certificate issued by the home regulator. This alleviated procedure is not available to financial institutions that are not subsidiaries of EU credit institutions because they are not able to obtain a certificate from their home regulator. Such institutions need to establish a Bulgarian entity and register it in the register of financial institutions maintained by the Bulgarian National Bank or provide services from their seat on a non-solicited and irregular basis.

The industry-specific passporting procedures, notifications and documental requirements vary for the different regulated industries but are generally available for EU-licensed institutions.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

A fintech company licensed in another EEA member state may passport its activity in Bulgaria and thus would be able to provide services through a branch or directly. In general, a fintech company licensed in a third country needs a licence from a Bulgarian regulator.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

In general, marketing of regulated services or activities shall be performed only by an entity that is licensed for such services and activities.

Marketing of financial instruments is subject to the regulatory framework set out in Directive 2014/65/EU on markets in financial instruments. Pursuant to the Markets in Financial Instruments Act, the information that the investment firms provide to their clients and potential clients, including in their advertising materials, must be correct, clear and not misleading. Advertising materials of investment firms must be clearly designated as such.

Marketing of crowdfunding performed in Bulgaria must be made in the Bulgarian language.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

At present, there are no such domestic regulations. Regulation (EU) 2022/858 on Distributed Ledger Technology Market Infrastructures (DLTR) which sets out a pilot regime for the regulation of crypto-assets that qualify as financial instruments within the Union applies (with some exceptions) as of 23 March 2023. The DLTR defines 'distributed ledger' as an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism. DLT financial instruments are defined as financial instruments issued, recorded, transferred and stored using distributed ledger technology.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

At present, Bulgarian law does not specifically regulate cryptocurrencies, except for the purposes of anti-money laundering measures. Implementing Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, Bulgarian law defines virtual currencies and custodian wallet provider and provides for registration of providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, with the National Revenue Agency (NRA). These providers are obliged entities under the AML legislation.

In addition, the NRA has issued non-binding interpretations on the tax treatment of mining and selling cryptocurrencies. As per these interpretations, cryptocurrencies are considered assets.

When services related to cryptocurrencies are performed as investment, ancillary services or activities under the Markets in Financial Instruments Directive (MiFID), including if financial instruments (such as, eg, contracts for differences (CFDs) or derivatives) are based on cryptocurrencies (namely, a cryptocurrency is the underlying asset of the financial instrument), all requirements of MiFID as implemented in Bulgaria would apply, including the licensing requirements.

If any services related to cryptocurrencies should be qualified as regulated services or activities under CRDIV (Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC), MiFID, PSDII (Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC) or e-money European regulations (collectively, the European Legislation), the respective requirements and restrictions of the European Legislation, which have been implemented in Bulgaria, would apply.

We are not aware of any proposed future developments in cryptocurrency regulation at the national level in Bulgaria.

The EU Markets in Crypto Assets Regulation will apply in Bulgaria from its effective date (estimated within the second half of 2024).

Read this article on Lexology

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

No.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

No. At the end of 2020, the Bulgarian government adopted the Concept Document for the Development of Artificial Intelligence in Bulgaria until 2030. This document clearly shows that Bulgaria prefers to avoid over-regulation (so as not to hamper innovation) and is inclined to leave the regulation of the use of artificial intelligence primarily in the hands of the institutions of the European Union, while dedicating its efforts to the adoption of national transposition measures.

For instance, a draft law for the amendment of the Copyright and Neighbouring Rights Protection Act submitted to the Bulgarian parliament in April 2023 aims at transposing into national law the EU DSM Directive 2019/790 providing for certain exceptions allowing for the use of data to train artificial intelligence. However, as of 31 May 2023, said draft has not yet been passed into law.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

The direct and indirect acquisition or increase of qualified participation or control (namely, more than 10, 20, 33 or 50 per cent of the total shares or voting rights) in credit institutions, investment intermediaries and insurance companies (and with some variations – in other regulated entities) require preliminary authorisation by the competent Bulgarian regulator, subject to restrictions on the right to exercise voting rights until such authorisation is obtained or either invalidity or an obligation to transfer the acquired participation in the case no authorisation is obtained.

In particular, prior authorisation by the Bulgarian National Bank is required for direct or indirect acquisition of a qualified participation or control in a credit institution. Such authorisation is granted following notification and submission of supporting documents to the Bank Supervision Department of the Bulgarian National Bank in line with the Credit Institutions

Act and the European Banking Authority's Guidelines, within 60 days of the receipt of confirmation from the regulator that the notification and the necessary documents are in place.

In extraordinary and objectively occurred circumstances when the acquisition was made before the filing of a notification (eg, at a stock exchange or indirectly as a result of parent acquisition, a business combination or in cases of corporate reorganisations), the notification may be filed after the acquisition but the acquirer may be prevented from exercising the voting rights until approved by the regulator or the regulator may impose compulsory measures – to restrict the exercise of voting rights or to instruct the sale to diminish the acquirer's share participation.

Respectively, a prior authorisation is required for the direct or indirect acquisition or increase of a qualified participation in an investment intermediary or an insurance company. The procedure is similar to the procedure applicable to the authorisation of the acquisition of a qualified participation or control of credit institutions, save that the competent regulatory authority is the Financial Supervision Commission (FSC), the Investment Activity Supervision Department (for investment firms), and respectively the Insurance Supervision Department (for insurance and reinsurance companies).

The terms for the authorisation, as well as the consequences of failure to file and receive authorisation, are similar to those applicable to credit institutions. In particular, if the acquisition of a qualified participation and control in an insurance company is made despite a prohibition issued by the FSC, the FSC is entitled to seek invalidation of a decision of the general meeting of shareholders.

A specific instrument to prevent violation of regulatory approval requirements in the case of a direct acquisition of shares in banks and insurance companies is the requirement to submit an opinion to the Central Depositary (banks and insurance companies in Bulgaria issue book-entry shares that are registered in the Central Depositary) issued by the respective regulator (the Bulgarian National Bank or the FSC) on the acquisition before the transfer of shares is registered in the Central Depositary.

In the case of other regulated entities such as financial institutions or insurance brokers, the notification follows the acquisition and does not per se prevent the exercise of voting rights.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Corruption and bribery represent general criminal offences under the Bulgarian Criminal Code. The Bulgarian Criminal Code also provides for a number of provisions pursuing financial crimes (crimes against the financial and credit system) and cybercrimes. The Criminal Code provides as well that the conduct of a regulated business without a licence or permit when such licence or permit is required constitutes a criminal offence.

In addition to the criminal offence in cases of corruption, there is a special act of general application aimed at pursuing corruption and providing for civil confiscation of the benefits of crimes separately from the confiscation as a penalty under the Criminal Code.

Regulated fintech companies (credit, payment or e-money institutions, investment intermediaries, insurance companies or insurance brokers) established in Bulgaria, including digital currency exchanges and digital currency custody services providers registered with the National Revenue Agency, are required to apply the Bulgarian anti-money laundering and combatting of terrorism financing legislation, as well as specific sanctions under the EU Sanctions regulations.

The anti-money laundering provisions set out in the Bulgarian Measures against Money Laundering Act and the measures on combatting terrorism financing set out in the Measures Against the Financing of Terrorism Act apply accordingly.

Financial sector institutions are required to adopt and apply internal rules and apply respective measures to prevent money laundering (customer due diligence and transaction due diligence involving client identification and verification of identification, collecting and safeguarding documents on the purposes and sources of financing, the origin of fund establishment and reporting to the Bulgarian financial intelligence unit – the Financial Intelligence Directorate to the State Agency National Security – in cases of suspicious clients and suspicious transactions).

Financial sector institutions are also obliged to apply measures aimed at preventing of financing of terrorism. They are obliged to freeze the assets of specifically listed persons. Respective sanctions regimes are also applicable either generally or particularly by the respective financial sector institutions, depending on the type and legal grounds of the respective restrictive measures.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no national regulatory or industry anti-financial crime guidance designed in particular for fintech companies although some guidance documents exist, for example, for credit institutions (by the European Banking Authority).

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The main legislative act on personal data protection in the European Union is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of

such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)), which became directly applicable in Bulgaria as of 25 May 2018.

Rules supplementing the GDPR can be found in the Bulgarian Personal Data Protection Act, which contains a few local rules on data protection and ensures the effective enforcement of the GDPR by the local supervisory authority – the Bulgarian Commission on Personal Data Protection.

The rules on personal data protection do not apply to anonymous or anonymised data as it does not relate to identified or identifiable natural persons and therefore does not constitute personal data.

Bulgarian law does not have significant deviations from the general EU-wide rules. As such, the processing of personal data must comply with the same basic rules and principles applicable within the European Union: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, accountability, privacy by design and by default. Processing of personal data is lawful when based on one of the expressly listed legal grounds: consent, contractual necessity, legal obligation, and legitimate interests, with an additional legal basis required for special categories of personal data. The GDPR imposes significant requirements in view of validity of consent – it must be freely given, specific, informed and unambiguous indication of the data subject's wishes given by means of a statement or by a clear affirmative action. Data subjects may benefit from the rights to request access to and rectification or erasure of personal data, or restriction of processing, to object to processing, to withdraw their consent to processing, to data portability, and to lodge a complaint with a supervisory authority.

It is notable that the GDPR imposes a significant burden on businesses in view of keeping detailed records of processing activities, notifying the authorities and affected data subjects regarding data protection breaches, carrying out detailed data protection impact assessments, and appointing a designated data protection officer. The transparency and accountability principles mentioned above also require significant effort in view of detailed notifications to data subjects and keeping documental proof of compliance with the requirements of the GDPR.

Non-compliance with the GDPR could result in administrative sanctions reaching up to €20 million, or up to 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

On the topic of international transfer of personal data to third countries outside the European Union and the European Economic Area, those are permissible in the following cases:

- If the European Commission has decided that the third country ensures an adequate level of protection. Such adequacy decisions have been issued with regard to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom and Uruguay.
- In the absence of an adequacy decision, the transfer of personal data is permissible if one of the following appropriate safeguards is implemented, as long as enforceable data subject rights and effective legal remedies for data subjects are available:

Read this article on Lexology

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules;
- standard data protection clauses adopted by the European Commission; currently, valid are the modernised standard contractual clauses adopted by means of Commission Implementing Decision (EU) 2021/914 of 4 June 2021;
- standard data protection clauses adopted by a supervisory authority and approved by the European Commission;
- an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; and
- an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

- In the absence of an adequacy decision or of appropriate safeguards, a transfer of personal data to a third country is permitted only in view of the following derogations for specific situations:

  - the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfer for the data subject due to the absence of an adequacy decision and appropriate safeguards;
  - the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
  - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
  - the transfer is necessary for important reasons of public interest;
  - the transfer is necessary for the establishment, exercise or defence of legal claims;
  - the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; and
  - the transfer is made from a register that according to law is intended to provide information to the public and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by law for consultation are fulfilled in the particular case.

- In all other cases, a transfer of personal data to a third country is permissible only if it is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller that are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. In such cases, the controller must inform the supervisory authority.

It is important to note that the decision of the Court of Justice of the European Union on *Schrems II* (Case C-311/18) has further raised the bar for the validity of data transfers to non-adequate third countries, both in view of carrying out a prior transfer impact assessment

Read this article on Lexology

and in implementing additional safeguards for the protection of personal data (encryption, pseudonymisation, etc). The European Data Protection Board has issued detailed recommendations on the expected compliance measures in this regard.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

The financial services sector is heavily regulated and cybersecurity provisions are already included in various laws and regulations, including those implementing PSD2, Markets in Financial Instruments Directive II and others.

The main pieces of cybersecurity legislation in Bulgaria are the Cybersecurity Act adopted in 2018 and the Ordinance for Minimal Requirements for Network and Information Security adopted in 2019. Those acts implement the NIS Directive with minimal derogations and deviations. They provide for the minimum specific requirements for network and information security that the obliged entities, providers of essential and digital services, public and regulatory authorities, and other providers of public services must observe to create a resilient and stable digital environment. Credit institutions (banks) are included in the list of providers of essential services that are obliged to implement cybersecurity measures as provided in the legislation.

In addition to the local legislation, in 2019, the European Banking Authority adopted 'Guidelines on ICT and security risk management'. The Guidelines establish requirements for credit institutions, investment firms and payment service providers on the mitigation and management of their information and communication technology risks and aim to ensure a consistent and robust approach across the single market. Those are generally applicable to payment and e-money institutions.

Insurance companies are under statutory obligation to observe the IT security requirements under the European Insurance and Occupational Pensions Authority (EIOPA) 'Guidelines on information and communication technology security and governance' (EIOPA-BoS-20-600). The Bulgarian Financial Supervision has issued special guidance in this respect.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

There are legal requirements on outsourcing by financial services companies of key functions or material aspects of their business in the applicable Bulgarian laws (eg, the Payment Services and Payment Systems Act). Although there are no national regulatory guidance documents, Bulgarian regulators strictly apply and follow the EU industry guidance documents such as those adopted by the European Banking Authority (EBA), the European

Securities and Markets Authority and the European Insurance and Occupational Pensions Authority (EIOPA).

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

At the national level, there are no specific legal requirements or regulatory guidance for the use of cloud computing in the financial services industry.

It should be noted, however, that the bank supervision authorities have quite broad powers to request and collect information from financial institutions, including to perform on-site inspections. They have the right to free access to all IT systems and offices of financial institutions. Those inspection rights apply also to the IT systems and offices of the subcontractors and service providers, including providers of cloud-based services.

Operators of essential services and key digital service providers, such as search engines, cloud computing services and online marketplaces have to comply with the security and notification requirements under the Cybersecurity Act.

Credit institutions are also strongly recommended to comply with the EBA Recommendations on outsourcing to cloud service providers. The recommendations are intended to clarify the EU-wide supervisory expectations if institutions intend to adopt cloud computing.

Insurance companies are obliged to follow the EIOPA 'Guidelines on outsourcing to cloud service providers' (EIOPA-BoS-20-002).

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Computer programs and databases are subject to copyright protection under the Bulgarian Copyright and Neighbouring Rights Act. Computer programs are protected as literary works and the protection applies to the expression of a computer program in any form. Ideas and principles that underlie any element of a computer program, including those that underlie its interfaces, are not protected by copyright.

Bulgarian law does not provide for a copyright registration regime or any other administrative measures for the copyright to occur. Copyright arises automatically from the moment of creation of the work, provided that the computer program is original, in the sense that it is the author's own intellectual creation and is fixed in tangible form.

Business methods and computer programs as such are not patentable under Bulgarian law. Under certain circumstances, computer-implemented inventions may be subject to patent protection if the patent claims show the presence of a technical effect.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

As a general rule, the holder of the copyright is the author (namely, the natural person whose creative efforts have resulted in the creation of the respective work). However, as an exception to this rule, the Bulgarian Copyright and Neighbouring Rights Act explicitly provides that, unless agreed upon otherwise, copyright in computer programs and databases developed under an employment contract shall belong to the employer. This means that the copyright in software is acquired by the employer with the mere fact of creation of the software (namely, it occurs automatically and no transferring is required to take place).

If the employees in the course of their employment develop any works subject to copyright protection that are different from software and databases (non-software works), then the applicable rule is that the copyright belongs to the employee who created the work (the author). In this case, by operation of law, the employer has the exclusive right to use the product for its purposes that are in line with its usual activities, without the consent of the author and without paying compensation to the author. In practice, this means that the employer cannot obtain the full title in such works but has an exclusive statutory worldwide licence to use the product for its purposes that are in line with its usual activities.

The above provisions, however, do not apply if the computer programs or other copyrightable works are developed by contractors or consultants. In such a case, the general rule is that, unless agreed upon otherwise, the holder of the copyright would be the author, and the ordering party may only use the work without the permission of the author for the purposes for which it was ordered. Therefore, in cases of works created by contractors or consultants the intellectual property matters should be dealt with in a contract that should clearly allocate the ownership and the rights of use of the IP assets developed under such cooperation.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

In cases of works subject to copyright protection (including software) created by a group of natural persons jointly, the general rule is that the exclusive rights are owned jointly, irrespective of whether the works constitute one indivisible whole or consist of separate parts each having individual significance. The consent of all co-owners is required for any modification of the work or for granting a licence for the use of the work. If the co-owners fail to reach agreement among themselves, the issue is to be resolved by the court. The licence fee due to the authors for the use of their work shall be distributed among them in shares by mutual agreement. In the absence of an agreement, it shall be considered that all the joint

authors' shares are equal. In the case of disputes, individual shares shall be determined in court in accordance with the contribution of each of the authors.

In cases of co-ownership of inventions and patents, unless otherwise agreed, each owner may use the invention, but the patent may be assigned or licensed only with the consent of all co-owners.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

The Trade Secrets Directive (EU) 2016/943 was implemented in Bulgaria by means of the Trade Secret Protection Act, in force as of 5 April 2019.

Apart from the civil law protection introduced by the above Act, trade secrets are also protected under the unfair competition law. In line with the Trade Secrets Directive the Bulgarian Trade Secret Protection Act provides for a legal definition of the term 'trade secret'. According to this definition, any information is a trade secret if it meets the following requirements:

- it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- it has commercial value because it is secret; and
- it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

The most notable element is the reasonable measures that the trade secret owners are required to implement to identify and protect their trade secrets. If companies are unable to show that such steps have been taken, the information may lose its trade secret status. The case law of the Bulgarian courts provides useful guidance with regard to the adequacy of such 'reasonable steps'.

The law protects trade secrets against direct unlawful acts – the acquisition, use or disclosure as well as against indirect infringements. The legal remedies available to trade secret owners in the case of unlawful action are generally the same as the legal remedies in cases of IP infringements (namely, stopping the unlawful use and further disclosure of misappropriated trade secrets; removal from the market of goods that have been manufactured on the basis of a trade secret that has been illegally acquired; and right to compensation for the damages caused by the unlawful use or disclosure).

As for the protection of trade secrets in court proceedings, the Bulgarian Trade Secret Protection Act sets forth a special set of rules in this respect. Upon a duly reasoned application by an interested party, the court may take specific measures to preserve the confidentiality of any trade secret or alleged trade secret used or referred to in the course of legal proceedings. In particular, the court may impose the following measures: restricting access to any document containing trade secrets; restricting access to court hearings and to relevant records and minutes by ruling the case to be examined or certain actions to be

performed *in-camera*; making available a non-confidential version of any judicial decision, in which the passages containing trade secrets have been removed or redacted. The court may not restrict access to the information to the persons who are parties to the proceedings and their procedural representatives. However, these persons are obliged to keep the relevant information confidential, otherwise, they will be subject to a fine to be imposed by the court.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brands can be protected either by registration of national trademarks with the Bulgarian Patent Office or by registration of EU trademarks with the EU Intellectual Property Office. Certain logo designs may also be protected by copyright as artistic works.

Prior to launching their brand or choosing their company name to be used on the local market, fintech businesses should conduct due diligence, including clearance searches in the databases of the Bulgarian Commercial Registry and the databases of the Bulgarian Patent Office and the EU Intellectual Property Office to make sure that the respective brand or company name are not in conflict with earlier third- party rights and are available for registration and use.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

There are various remedies against infringements of intellectual property rights under Bulgarian civil and criminal law.

The main remedy is filing a civil litigation case for IP rights infringement where the right holder may request from the court to:

- establish the infringing activity;
- issue against the defendant an injunction prohibiting the continuation of the infringement;
- order the destruction of infringing goods; and
- award compensation for the damages suffered by the plaintiff as a result of the infringement.

In the course of such litigation, it is also possible to file a request for preliminary injunctive measures, such as prohibition on a provisional basis of the continuation of the infringement.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

The fintech industry has not been the focus of attention of the Bulgarian competition enforcement authorities yet, and there are no notable local cases and precedents specific to fintech.

That said, in line with the trends in the rest of Europe, the Bulgarian competition authority is showing increasing interest in the digital economy. An illustration of this is the recently initiated sector inquiry into the e-commerce sector, which matches a similar sector inquiry conducted at the EU level previously, by the European Commission.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

There are no specific tax incentives applicable to the fintech companies. They could benefit from some of the general tax exemptions such as:

- accelerated amortisation of the products created for the company as a result of research and development activities of scientific institutes in connection with the main object of activity of the company – the value of the asset could be 100 per cent deducted from the company's financial results during the year of the acquisition of the asset;
- payment of scholarships to university students – these are recognised as company expenses (subject to certain conditions); and
- hiring of unemployed people – possibility to reduce the financial results for corporate income tax purposes by the amounts paid as salary and social security contributions (certain conditions apply).

Apart from the tax incentives, investments in startups or in existing businesses leading to certain positive results for the economy could be subject to other forms of incentives. An investment in a startup or expansion of an existing business operating in the field of creation of computer program products, activities in the IT field or the provision of information services could become subject to such incentives. The incentives could include various measures, such as accelerated administrative processing in relation to certain administrative processes (often irrelevant to startups in the IT sector that are not to acquire or build buildings) as well as financial incentives (eg, partial compensation of the expenses incurred in connection with the salaries paid to the newly hired employees, such as social security and medical security expenses or payment of scholarships to the newly recruited employees to complete their education or acquire professional qualification). The provision of different incentives is subject to numerous conditions.

Read this article on Lexology

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

To the best of our knowledge, Bulgaria is not to develop its own initiatives regarding digital taxation, fintech businesses included. Most likely, if a political decision within the European Union is reached, Bulgaria would follow the rules and policies so determined. However, we could not find any position paper or statement by the Bulgarian government that could shed light on this topic.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

Citizens of countries within the European Economic Area and Switzerland are entitled to enter and stay in Bulgaria for three months without the necessity to complete any immigration procedures. They are entitled to work for a Bulgarian company and no work authorisation is required. If they intend to stay for more than three months in Bulgaria, they can obtain long-term residence certificates with a term of validity of up to five years.

As a rule, citizens of countries outside the European Economic Area and Switzerland (namely, third-country nationals) may reside and work in Bulgaria only after completion of certain work and residence authorisation procedures.

There are different types of work and residence authorisation procedures for third-country nationals depending on the duration of the intended assignment in Bulgaria, payroll country, qualification of employees, etc.

The most popular type of permit used in Bulgaria by companies for hiring highly skilled employees is the EU Blue Card.

The application for the EU Blue Card must be sponsored by a Bulgarian company and the entire process includes the following steps:

- the Bulgarian company files an application for work and residence authorisation for each employee with the migration authorities in Bulgaria;
- after approval of the work and residence application by the migration authorities in Bulgaria, the employee must apply for a long-term Bulgarian visa at the Bulgarian Embassy in their home country; and
- after the employee comes to Bulgaria with a long-term Bulgarian visa, the employee obtains a work and residence permit card – the EU Blue Card, from the migration authorities in Bulgaria.

The entire process takes three to four months and the employee is entitled to start working for the Bulgarian company after the completion of all steps and the issuance of the EU Blue Card. The term of validity of the EU Blue Card is five years and can be renewed for new five-year terms without limitation.

Bulgaria also started the introduction of a start-up visa programme for high-tech and innovative projects, but regulations are yet to be adopted to implement the programme. The start-up visa would be available only to shareholders of Bulgarian companies and not to employees.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

An encouraging trend that could be noted in recent years is the increasing involvement and support of competent regulators in the fintech sector. The Bulgarian National Bank has shown noticeable flexibility and support in the procedures for licensing of new e-money institutions and has maintained a productive environment for ensuring compliance with the legal requirements for licensing while at the same time maintaining very high supervisory standards.

The Financial Supervision Commission adopted and currently implements a specific Strategy for Monitoring Financial Innovations (FinTech) in the Non-banking Financial Sector in the period 2021–2024. In brief, the strategy sets four main goals in this field:

- establishment of a secure and measurable regulatory environment in which fintech companies can operate, including with respect to the offering of financial products and services or offering of products of entities under the supervision of the regulator;
- analysis and taking of respective regulatory measures for securing safety, stability of the financial services market and protection of the consumers using financial services;
- development of the Innovation Hub – an initiative aiming to establish an effective two-way communication channel between non-banking institutions developing innovative financial services and the regulator; and
- monitoring the development of sandbox regimes and taking measures for their possible implementation by the regulator.

* *The authors wish to thank Alexander Chatalbashev, Peter Petrov, Nedyalka Novakova and Deyan Terziev for their assistance in the preparation of this chapter.*

Read this article on Lexology

BOYANOV & Co.

Damian Simeonov	d.simeonov@boyanov.com
Nikolay Zisov	n.zisov@boyanov.com
Svetlina Kortenska	s.kortenska@boyanov.com
Georgi Drenski	g.drenski@boyanov.com
Stela Sabeva	s.sabeva@boyanov.com

82 Patriarch Evtimii Boulevard, Sofia 1463, Bulgaria
Tel: +359 2 8 055 055
www.boyanov.com

Read more from this firm on Lexology

Read this article on Lexology

Canada

Alix d'Anglejan-Chatillon, Ramandeep Grewal, David Elder, Shawn Smith and Éric Lévesque*
Stikeman Elliott LLP

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES	**81**
General innovation climate	81
Government and regulatory support	82
FINANCIAL REGULATION	**83**
Regulatory bodies	83
Regulated activities	83
Consumer lending	84
Secondary market loan trading	84
Collective investment schemes	85
Alternative investment funds	85
Peer-to-peer and marketplace lending	85
Crowdfunding	86
Invoice trading	86
Payment services	87
Open banking	87
Robo-advice	88
Insurance products	88
Credit references	88
CROSS-BORDER REGULATION	**89**
Passporting	89
Requirement for a local presence	90
SALES AND MARKETING	**90**
Restrictions	90
CRYPTOASSETS AND TOKENS	**91**
Distributed ledger technology	91
Cryptoassets	91
Token issuance	92
ARTIFICIAL INTELLIGENCE	**92**
Artificial intelligence	92
CHANGE OF CONTROL	**93**
Notification and consent	93
FINANCIAL CRIME	**93**

Read this article on Lexology

Anti-bribery and anti-money laundering procedures 93
Guidance 94

DATA PROTECTION AND CYBERSECURITY 94
Data protection 94
Cybersecurity 95

OUTSOURCING AND CLOUD COMPUTING 96
Outsourcing 96
Cloud computing 97

INTELLECTUAL PROPERTY RIGHTS 97
IP protection for software 97
IP developed by employees and contractors 97
Joint ownership 98
Trade secrets 98
Branding 98
Remedies for infringement of IP 99

COMPETITION 99
Sector-specific issues 99

TAX 99
Incentives 99
Increased tax burden 100

IMMIGRATION 101
Sector-specific schemes 101

UPDATE AND TRENDS 101
Current developments 101

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Canadian fintech industries, particularly digital payments, digital trading, robo-advising and open banking, continued to experience significant growth until 2022. The pace of innovation had been accelerated by expansive fintech-supportive regulation at the provincial and federal level, changing consumer patterns during the covid-19 pandemic, and investment in fintech start-ups and in-house labs by leading Canadian financial institutions. While Canadian financial institutions have led the charge in many cases, fintech start-ups are now a key component of the fintech ecosystem across the country. Developments included major investments in artificial intelligence (AI)-driven fintech solutions, blockchain, regtech, and – in the insurance industry where Canada is a significant global player – in insurtech.

As in other jurisdictions globally, headwinds in the tech market and the broader post-pandemic inflationary pressures and economic downturn have created a more challenging environment for fintech innovation in the Canadian market.

In the cryptocurrency sector, Canadian regulators have shown leadership in mapping a framework and pathway to regulation designed to address both high-stakes industry developments and investor protection by issuing Staff Notice 21-329 – Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements (SN 21-329) and approving crypto-based retail investment fund launches subject to novel terms and conditions. The full impact of the current turmoil in the crypto market, which has recently been amplified by the collapse of FTX and the bankruptcies of crypto lenders BlockFi, Voyager Digital and Celsius Network, and other dominant stakeholders, has yet to fully play out in the Canadian crypto ecosystem. However, the expectation is that Canadian regulators will shift the focus more squarely onto investor protection over innovation until the market stabilises and stakeholders become fully regulated or exit the market.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Canadian governments, major financial market stakeholders and key regulators recognise the importance of fintech and have actively encouraged investment and innovation in the sector. Regulatory initiatives to date include:

- regulatory sandbox and launchpad programmes administered by securities regulators that allow fintech start-ups to test products and business models without the usual regulatory restrictions, and more flexibility to raise capital through new and more flexible prospectus exemptions, including crowdfunding exemptions;
- fintech cooperation agreements with several foreign jurisdictions;
- retail payments oversight and a licensing framework under the Retail Payments Activities Act (Bill C-30, An Act Respecting Retail Payment Activities, 2nd Sess, 43rd Parl, 2021, cl 177 (assented to 29 June 2021 and partly in force);
- federal regulatory and support initiative for open banking or consumer-driven finance;
- notices and an actionable roadmap by the Canadian Securities Administrators guiding the services and uses related to cryptocurrency and cryptoassets; and
- where applicable, derivatives law requirements in the cryptocurrency sector.

There continues to be a focus across the country on collaboration between Canadian core financial institutions, fintech start-ups and regulators. Regional governments in Canada's major cities have developed AI hubs and super-clusters, such as in Montreal, where the Quebec government has earmarked C$100 million over five years for the development of AI and fintech industry growth. Additional academic and local government funding initiatives have also multiplied across the country.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

Canada's provincial and territorial securities administrators are the primary regulators of fintech financial products and services relating to capital markets (including crypto assets). They work together under one umbrella as the Canadian Securities Administrators (CSA), together with the Canadian self-regulatory organisation that governs securities dealers, the Investment Industry Regulatory Organization of Canada (IIROC), which has been restructured to become the New Self-Regulatory Organization of Canada (New SRO), effective from 1 January 2023. At the federal level, the Office of the Superintendent of Financial Institutions (OSFI) is responsible for the supervision and regulation of banks, insurance companies and trust and loans companies and has highlighted the need for resilient technology infrastructures. The Canada Revenue Agency and its various provincial counterparts have also developed and published policies or guidance on fintech-related matters. The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Canada's federal anti-money laundering (AML) authority, also regulates certain fintech products and services, including money services businesses (MSBs) dealing in fiat and (or) virtual currencies. The Bank of Canada (BoC), Canada's central bank, closely monitors fintech developments and distributed ledger technologies and has been appointed as the oversight body for the new retail payments regime under the Retail Payments Activities Act (RPAA). As with other leading central banks, it is developing a cash-like central bank digital currency as a further contingency given the rapid decline in the use of cash and the explosive growth of digital payments. A number of other fintech initiatives are also administered at the local level by various municipal governments.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Fintech businesses may be subject to various provincial licensing requirements under applicable provincial securities and derivatives laws to the extent that they engage in activities or facilitate transactions in securities or derivatives. These rules also govern trading in cryptoassets that are regulated as securities and those that are not but where the manner in which these assets are traded and held constitute 'crypto contracts', such that the instruments are treated as 'investment contracts' and therefore 'securities'. The rules include dealer and adviser registration for entities or persons considered to be trading or advising in securities or derivatives for a 'business purpose' and related compliance obligations. The management of investment funds also triggers the application of investment fund manager registration requirements in certain situations. Businesses undertaking initial coin offerings or initial token offerings may also be subject to prospectus or product qualification requirements or compliance with related exemptions.

Associated regulations require compliance with know-your-client (KYC) and know-your-product rules, suitability, insurance, financial and customer reporting, custody requirements and cybersecurity risk management protocols, among other requirements. Given the traditional definition of 'exchange' or 'marketplace' (namely, an entity that brings together

multiple buyers and multiple sellers of securities or derivatives), the CSA requires that fintech businesses involved in cryptocurrencies also consider whether they must be registered as exchanges or alternative trading systems.

In addition, both foreign and domestic MSBs must register with FINTRAC and comply with KYC, reporting, record-keeping, travel rule and compliance programme requirements. MSBs include businesses that deal in fiat and virtual currencies and foreign exchange. MSB registration may also be required in Quebec under MSB legislation in that province.

A number of other fintech-related activities, including lending, factoring, invoice discounting, secondary market loan trading, providing yield-generating products, and deposit-taking and trust company-type activities may be subject to a number of different regulatory requirements, depending on the relevant features of the business.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Consumer lending is not as highly regulated in Canada as in certain other jurisdictions. Nevertheless, aspects of consumer lending are regulated in Canada at both the federal and provincial levels. At the federal level, the regulation depends on the regulated status of the entity providing consumer credit. Banks and other financial institutions have cost-of-borrowing disclosure obligations for mortgages, credit cards and certain other types of credit. Criminal interest rate provisions in the Criminal Code (RSC 1985, c C-46) preclude the effective annual interest rate for an advance of credit from exceeding 60 per cent per year. No distinction is drawn between commercial and consumer contracts in this regard, though certain low-value (payday) loans are exempt.

Provincially, payday lenders are subject to a licensing requirement in most provinces. In addition, provincial consumer protection legislation in New Brunswick, Nova Scotia, Quebec and Saskatchewan imposes a lender licensing requirement (or permit or registration requirement) for consumer lending. A number of provinces have implemented or are in the process of implementing high-cost credit legislation, which can impose a licence or registration requirement.

Secondary market loan trading

6 | Are there restrictions on trading loans in the secondary market in your jurisdiction?

The regulation of trading loans in the secondary market depends on whether the loan instruments would be regarded as securities (namely, under a multi-factor test to determine if the particular loan instrument is an 'investment contract' or 'a bond, debenture, note or other evidence of indebtedness'). Loans acquired on the secondary market are much more likely to be characterised as securities than originated loans.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Collective investment schemes, generally referred to as 'investment funds' under Canadian securities regulations, are primarily subject to provincial securities laws. Investment funds include non-redeemable (or closed-end) funds as well as mutual funds. Primarily, persons operating or administering collective investment structures (including those that hold or invest in virtual currencies or that provide alternative finance products or services) may also be subject to investment fund manager registration requirements, in addition to dealer, adviser and prospectus or private placements requirement. The structures themselves may also be subject to the reporting and conduct requirements that apply to investment funds, including under National Instrument 81-102 – Investment Funds (NI 81-102), and National Instrument 81-104 – Alternative Mutual Funds (NI 81-104) (which applies specifically to retail alternative funds), National Instrument 81-106 – Investment Fund Continuous Disclosure (NI 81-106) and a number of other instruments, including, depending on the nature of the regulated intermediary, IIROC rules and, in the case of mutual fund dealers, the rules of the Mutual Fund Dealers Association of Canada, which, effective from 1 January 2023, will be merged with IIROC into the New Self-Regulatory Organization of Canada (New SRO).

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Yes. Any person or company acting as a manager of an investment fund must register as an investment fund manager and comply with registration and related requirements, or rely on certain exemptions. This requirement is triggered in the provinces of Ontario, Quebec, and Newfoundland and Labrador if the fund has investors resident in that province. Across Canada, investment by Canadian investors in investment funds is subject to provincial prospectus requirements and, in the case of private placements, related exemption requirements, as well as dealer registration requirements and regulations that govern the content and delivery of offering documents and post-trade reports. Under securities legislation, these obligations apply to both managers of conventional investment funds, as well as alternative investment funds (AIFs). Domestic retail funds are also subject to additional regulations under NI 81-102 and NI 81-106, with AIFs permitted to engage in a broader range of investment strategies (eg, including more latitude to engage in short-selling, borrowing and the use of derivatives) than is permitted for conventional investment funds.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Peer-to-peer (P2P) lending businesses in Canada may be subject to registration as dealers with the provincial securities regulators in the provinces in which they operate. As a result, P2P lenders may also be required to comply with prospectus and other regulatory requirements applicable to any other securities dealer operating in the same jurisdiction, including

restricting investing opportunities to qualified accredited investors. Other provincial entities have enlisted the help of affiliated companies to issue notes and agreements on a prospectus-exempt basis. Additionally, some P2P lenders have obtained exemptions from certain requirements such as prospectus filing obligations through existing exemptions under the provincial securities legislation.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

Fintech companies that raise capital through crowdfunding are subject to provincial securities regulations. Various provincial securities regimes have adopted crowdfunding prospectus exemptions through a range of regulations and instruments. For example, the Ontario Securities Commission adopted Ontario Instrument 45-506 – Start-Up Crowdfunding Registration and Prospectus Exemptions, which provided specific registration and prospectus exemptions for start-up crowdfunding companies.

Similar regimes have also been adopted in other provinces through, among others, Multilateral Instrument 45-108 – Crowdfunding and Multilateral CSA Notice 45-316 – Crowdfunding Registration and Prospectus Exemptions permit early-stage companies and small businesses to raise limited amounts of capital through crowdfunding platforms. Both public and non-public companies are permitted to rely on the prospectus exemption. Also, where securities crowdfunding offerings are facilitated through a funding portal, the funding portal generally must be registered under National Instrument 31-103 – Registration Requirements, Exemptions and Ongoing Registrant Obligations (NI 31-103) and with the applicable provincial securities regulators.

The CSA published a new regulation, National Instrument 45-110 – Start-up Crowdfunding Registration and Prospectus Exemptions (NI 45-110), that contributes to a harmonised national framework and will replace similar instruments previously adopted by provincial securities regulators. NI 45-110 came into force on 21 September 2021.

On 14 February 2022, the federal government took the unprecedented step of invoking the Emergencies Act (Canada) to end disruptions, blockades, and the occupation of the city of Ottawa. These developments led to further action to limit the flow of financing of the blockades by extending the requirement to register as MSBs under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA, SC 2000, c 17), Canada's federal anti-money laundering legislation, to crowdfunding platforms and certain payment service providers that were not previously regulated for this purpose.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

There is no specific regulation in Canada of invoice trading. Depending on its characteristics, invoice trading may be subject to provincial securities laws and (or) FINTRAC obligations, to the extent it falls under the existing scope of securities trading activity or an MSB service, respectively. In addition, if carried out by a banking entity or an entity affiliated with a bank, it may be subject to federal banking legislation. Provincial loan and trust legislation may be

applicable if the services include extending loan and trust services to the public and provincial consumer protection laws may also apply.

Payment services

12 Are payment services regulated in your jurisdiction?

The continuation of the 2016 Payment Canada modernisation programme, amendments to the existing Payment Clearing and Settlement Act (PCSA, SC 1996, c 6), and the new RPAA, are expected to provide robust support and innovation opportunities for payment services in Canada. Payment services will continue to be subject to FINTRAC licensing to the extent that they are subject to MSB licensing requirements.

In December 2020, Payments Canada published the Modernization Delivery Roadmap, outlining the implementation process for two national payment systems enabled by the global ISO 20022 messaging standard: Lynx and the Real-Time Rail (RTR). Lynx, Canada's new high-value payments system, began operations on 30 August 2022, replacing the Large Value Transfer System (LVTS), which had operated since 1999. Lynx will enable payment and settlement finality and flexibility for the application of future technologies, as well as enhanced cybersecurity capabilities. The RTR will provide real-time irrevocable credit payments and allow fintech service providers to develop new and enhanced ways for individuals to pay for goods or services and transfer money. The RTR was set to launch in 2022 but its delivery has been postponed.

The RPAA will apply to all retail payment activities performed by payment service providers in Canada, as well as all activities performed by providers outside of Canada who provide retail payment activities to an end user within Canada. Under the RPAA, payment service providers will be required to register with the BoC. Certain retail payment activities, such as those performed by systems under the PCSA, payment functions performed by Payments Canada, the BoC or, other designated entities and activities, will be exempt from the new RPAA. The new requirements will be fleshed out in future implementing regulations.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

In August 2021, the federal government published its Final Report – Advisory Committee on Open Banking. The report, which focused on supporting innovation and competition in the Canadian financial services sector system, proposed a two-phased approach set to be completed by 2023.

The recommendations outlined a consumer-focused framework for implementing secure open banking in Canada. Under new regulations, such as those to be enacted under the Consumer Privacy Protection Act (part of Bill C-27, 1st Sess, 44th Parl, 2022, cl 2 (first reading 16 June 2022)), individuals would be granted more freedom to direct and transfer their personal information from one organisation to another, including to accredited third-party service providers. Other Canadian organisations such as the Canadian Competition

Bureau have also made strong recommendations to further modernise Canada's financial sector following consultations with industry and regulatory stakeholders in light of global developments in open banking. Further to amendments made under the PCMLTFA in 2022 discussed above, FINTRAC regulatory guidance was also amended to provide that certain types of payment service providers may also be subject to registration as MSBs under that legislation.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Companies engaged in robo-advising activities are subject to securities registration and related regulatory requirements in the governing province where the business operates, which are generally harmonised across the country under NI 31-103.

The CSA has also issued regular guidance, including Staff Notice 31-342 – Guidance for Portfolio Managers Regarding Online Advice, outlining the applicability of securities laws to online advisers. Fintech companies providing robo-advising are required to follow the same rules as human advisers, including complying with KYC and related requirements, and participating in due diligence and compliance reviews by CSA staff. The CSA has generally declined to grant exemptive relief for robo-advisers from NI 31-103 and related rules.

Pursuant to the proposed Consumer Privacy Protection Act (part of Bill C-27, 1st Sess, 44th Parl, 2022, cl 2 (first reading 16 June 2022)), organisations employing automated decision systems that assist or replace the judgement of human decision-makers would face new transparency obligations with respect to the nature of such systems and their potential impact on individuals. As of September 2023, Quebec's Private Sector Privacy Law (RSQ, cl 39.1) will impose a similar requirement. Bill C-27 will also enact the Artificial Intelligence and Data Act (cl 39), which would impose a number of obligations on artificial intelligence systems that are designed to avoid biased output and harm to individuals.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Fintech companies that provide insurance services are subject to the same regulations as conventional providers of insurance services, as well as broader legislation applicable to fintechs under Canadian AML, consumer protection and privacy legislation.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

There is no consolidated federal authority governing credit reference and information services. Both consumer protection legislation such as the Consumer Reporting Act (RSO

1990, c C-33), Personal Information Protection and Electronic Documents Act (PIPEDA, SC 2000, c 5) and its provincially-enacted counterparts, and individual contracts, govern the disclosure of credit information, activities related to credit cards and other credit agreements such as payday loans.

CROSS-BORDER REGULATION

Passporting

17 | Can regulated activities be passported into your jurisdiction?

Foreign fintech entities operate under the same regulatory framework as domestic businesses for regulated activities such as banking or insurance, to the extent their activities in Canada trigger regulation.

Provincial securities regulators have adopted a passport approach to the application of securities regulation under Multilateral Instrument 11-102 – Passport System.

This regime has been adopted by all provinces except for Ontario. It allows the participant to gain access to markets across Canada while dealing solely with their principal regulator and complying with harmonised regulation. Participants can clear a prospectus, obtain a discretionary exemption, register as a dealer or adviser in their home province and this decision or receipt is deemed to be a decision or receipt from other securities regulatory authorities, as long as conditions, such as filing requirements and fee payments, are met.

While Ontario is not a party to this system, it operates under a coordinated review model that generally allows for seamless administration through dealing with the regulator in the Canadian jurisdiction with which the entity has the greatest nexus. In certain limited areas of securities regulation, Canadian securities administrators may also recognise compliance with foreign regulations as a form of 'substituted compliance' and allow for exemptions or waivers on that basis. Canadian securities regulators have also entered into memoranda of understanding with various international regulators to allow for coordination in regulation, information sharing and enforcement.

Under NI 31-103, there is also a type of cross-border passporting that applies to permit non-Canadian dealers and advisers that satisfy certain conditions to engage in non-Canadian trading and advisory activities with qualified Canadian resident 'permitted clients' under the 'international dealer' or 'international adviser' exemptions, largely premised on the basis of having appropriate regulatory oversight in their home jurisdiction. A similar regime also exists for non-Canadian investment fund managers in certain provinces.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

Fintech companies are not per se subject to any licensing requirement. If they do need to be licensed, it is because their foreign regulatory status or activities in Canada may trigger the application of an existing licensing regime.

Fintech companies that are subject to foreign money services business registration are not required to establish a Canadian presence (although they must designate a local agent for service or process). Similarly, foreign businesses that are subject to dealer, adviser or investment fund manager registration are generally not required to establish a local Canadian entity to register or rely on filings-based exemptions (although they must also designate a local agent for service or process). Full-service investment dealer registration, however, does require that a Canadian subsidiary be established and staffed appropriately. With certain exceptions, federal banking and insurance regulation also requires that licensed entities establish a Canadian presence.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Marketing of financial services and products to Canadian users is subject to Canadian securities and derivatives laws. In particular, under provincial securities and derivatives legislation, a 'trade' is broadly defined to include 'any act, advertisement, solicitation, conduct or negotiation directly or indirectly in furtherance' of a trade in securities or derivatives and these activities may therefore be subject to dealer registration and prospectus requirements.

Marketing to Canadian users may also subject an entity to licensing with the Financial Transactions and Reports Analysis Centre of Canada as a money service business (MSB) or foreign money services business and to MSB registration in Quebec, as applicable. Marketing and advertising are also subject to provincial consumer protection legislation and generally, for Canadian banking and insurance purposes, an entity should not engage in targeted marketing to Canadian customers, particularly retail customers, unless that activity can be carried out in compliance with applicable licensing requirements.

The law known as Canada's Anti-Spam Legislation (SC 210, c 23) generally requires prior express consent for an organisation to send an email, text or other direct electronic message for marketing or promotional purposes. Telemarketing in Canada is regulated by the Unsolicited Telecommunications Rules, which include provisions requiring compliance with a national do-not-call list.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

The Canadian federal government has been experimenting with blockchain technology in various fields while the Bank of Canada (BoC) is conducting research on the effects of introducing a central bank digital currency. The BoC has noted that stablecoins, crypto assets backed fully or in part by currency-of-commodity holdings, have widespread potential. The BoC is further involved with Payments Canada and TMX Group on a research initiative, Project Jasper, which experiments with the use of distributed ledger technology for payments. VersaBank, a Canadian financial institution regulated by the Office of the Superintendent of Financial Institutions (OSFI), also announced plans to launch VCAD, a type of digital currency backed by bank deposits. However, the failure of the TerraUSD algorithmic stablecoin to keep its peg to the US dollar, the subsequent collapse of the Luna crypto network and the broader shocks in the crypto market in 2022 could lead to further regulatory initiatives in Canada specifically targeting the use of distributed ledger and blockchain technology in retail investment transactions.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

Virtual currencies are not treated as legal tender in Canada under section 8 of the Currency Act (RSC 1985, c C-52) and may be subject to Canadian provincial securities and derivatives laws to the extent that they are considered a security (including a 'crypto contract') or a derivative under that legislation.

The Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC) (or the New Self-Regulatory Organization of Canada) effective from 1 January 2023) have also acknowledged that it is widely accepted that certain well-established virtual currencies that function as a form of payment or a means of exchange on a decentralised network, such as bitcoin, are not currently in and of themselves, securities or derivatives. They are rather akin to an intangible commodity, the value of which fluctuates based on the market. In assessing whether a particular virtual currency will be considered a security subject to Canadian securities laws, the CSA will perform case-by-case, fact-dependent analyses and consider the substance of the virtual currency over its form. The CSA has adopted an investment contract test to apply to blockchain and cryptocurrency transactions that resemble traditional securities. In particular, the CSA has stated that the manner in which these assets are traded and held may constitute a 'crypto contract', such that the instruments should be regulated as 'investment contracts' and therefore as 'securities'.

Virtual currency transfer services are subject to money services business (MSB) registration with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), which

includes know-your-client, client identification, record-keeping, reporting and other anti-money laundering programme compliance requirements.

Currently, Canadian securities regulators have recognised or registered a number of domestic platforms or other intermediaries that facilitate trading in cryptoassets.

In August 2022, the OSFI, Canada's prudential banking regulator, also announced an interim approach for the regulatory capital and liquidity treatment of the crypto assets exposure of federally regulated financial institutions. In November 2022, the OSFI issued a further advisory, signalling its expectation that federally regulated financial institutions clearly understand the risks of any planned cryptoasset activities and ensure that these risks have been properly addressed, including by complying with existing federal financial laws in relation to cryptoassets, consistent with the principle endorsed by the Financial Stability Board, 'same activity, same risk, same regulation'.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Digital currency exchanges and brokerages may be subject to FINTRAC regulation as money service businesses (MSBs) (or in the case of non-Canadian exchanges or platforms, foreign MSBs or foreign money services businesses). These entities must follow specific obligations imposed by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (Canada) and associated regulations, including registration and compliance.

Digital currency exchange or brokerages may also be subject to provincial securities legislation, requiring registration as either a dealer platform or marketplace platform. Under Staff Notice 21-329 – Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements, entities are generally advised to register initially as 'restricted dealers', gradually transitioning to full investment dealer registration, and if applicable, marketplace recognition, depending on the nature or products or services they provide and the manner in which investment, trading and custody are handled.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

The regulation of artificial intelligence (AI) and robo-advisers will continue to be an area of development in the financial services industry, although the general direction is that the same registration, know-your-client and information requirements of conventional wealth managers and advisers can be applied to digital advisers. Importantly, online advisers must be registered with the Canadian Securities Administrators (CSA) before advising or dealing in securities unless an exemption is available.

Read this article on Lexology

Further, the registration and conduct requirements of NI 31-103 are technology-neutral and there are no online advice exemptions for AI portfolio managers (PMs). PMs must register prior to implementing their online advice operating model, after which the CSA will assess how the firm will meet its obligations under NI 31-103.

The proposed Artificial Intelligence and Data Act (part of Bill C-27, 1st Sess, 44th Parl, cl 39 (first reading 16 June 2022) would impose on operators of AI systems a number of restrictions and requirements designed to eliminate biased output and harm to individuals.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Money service businesses registered with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) must provide notice of any changes to information previously provided to FINTRAC in connection with such registration within 30 days of becoming aware of the change. Schedule 1 to the Registration Regulations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA, SC 2000, c 17) requires an applicant for registration to disclose every person, corporation or other entity that owns or controls, directly or indirectly, 20 per cent or more of the shares of the corporation.

The direct or indirect acquisition of 10 per cent or more of the securities of a registered securities firm, or all or a substantial part of its assets, is also subject to prior notification to securities regulators and, if applicable, approval of the Investment Industry Regulatory Organization of Canada (which will become the New Self-Regulatory Organization of Canada, effective from 1 January 2023) pursuant to its Dealer Member Rules and to disclosure of changes to upstream ownership. Regulated banks and insurance companies are similarly subject to pre-approval requirements for acquisition of significant interests, including change of control. The acquisition of significant positions in, or control of, publicly traded entities in Canada is also subject to securities laws and stock exchange rules. Depending on the size of the firm and nature of activities, Canadian antitrust and competition regulations may also impose notification or approval requirements.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Registered entities must comply with reporting, record-keeping, know-your-client (KYC) and other anti-money laundering or anti-terrorist financing (AML/ATF) compliance programme requirements. Securities dealers, life insurance companies, banks, brokers and agents, money services businesses and certain other financial businesses are subject to the AML

and ATF compliance requirements, including compliance programme, KYC, reporting, record-keeping and other requirements of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Additional requirements apply under the Criminal Code, the Corruption of Foreign Public Officials Act (SC 1998, c 34) and Canadian sanctions legislation.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

FINTRAC issues guidance on policy interpretations, transaction reporting, record-keeping and other obligations for reporting entities. Fintech companies, among others, that qualify as either money service businesses or securities dealers have specific guidelines as to registration, reporting and regulatory compliance.

The Royal Canadian Mounted Police (RCMP), as a member of the Financial Crimes Task Force, sets standards and promotes the implementation of measures to combat money laundering, terrorist financing and other threats to the international financial system. The RCMP is also responsible for enforcement of the Criminal Code.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

There are four general privacy and data protection statutes in Canada governing the processing and transfer of data: one federal and three substantially similar provincial statutory regimes (Alberta, British Columbia and Quebec).

The federal law, Personal Information Protection and Electronic Documents Act (PIPEDA), applies to fintech providers that operate within any of the industries that are federally regulated – most notably (in this context) the banking industry. PIPEDA applies to the processing of personal information in the course of commercial activity in any province that has not enacted its own privacy laws and to inter-provincial and international disclosures of personal information. Consequently, many national fintech service providers may be subject to PIPEDA, even if they are located in one of the three provinces with its own legislation.

Privacy laws generally permit the storage or processing of personal information outside of Canada, with consent. For the least sensitive types of personal information, implied consent is often sufficient (namely, posting a notice or including a disclosure in an organisation's privacy policy). For more sensitive personal information, Canadian privacy laws may require express consent to such transfers.

As of September 2023, Quebec's Private Sector Privacy Law (RSQ, c P-39 1) will also explicitly require that an organisation conduct an impact assessment with respect to any transfers of personal information outside of that province.

Read this article on Lexology

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

In Canada, cybersecurity laws and regulations were typically established in the context of personal information protection. Methods of protection include physical, organisational and technological measures and aim to safeguard against loss, theft, unauthorised access, disclosure, copying, use and modification. In assessing the adequacy of security measures implemented by an organisation, the privacy commissions often look for an implementation of recognised third-party certifications and standards that are appropriate for the organisation's industry.

Canadian regulators and self-regulatory organisations (including the Canada Securities Administrators (CSA), Investment Industry Regulatory Organization of Canada (IIROC), Office of the Superintendent of Financial Institutions (OFSI) and the Mutual Fund Dealers Association of Canada) have issued a considerable amount of fintech-specific cybersecurity guidance on cybersecurity best practices, including:

- corporate cybersecurity policies;
- incident response plans and reporting;
- employee cybersecurity training; and
- risk assessment and management (including vendor risk management).

While non-binding, this guidance is widely followed by the organisations to which it applies.

Unlike many other jurisdictions, Canada has not yet adopted comprehensive cybersecurity rules that legally require financial services companies, including those in the fintech sector, to adopt best practices of the type just described, although a new Critical Cyber Systems Protection Act (Bill C-26, 1st Sess, 44th Parl, cl 13 (first reading 14 June 2022)) is before Parliament at the time of writing. It would require operators of critical systems to establish a cybersecurity programme, report breaches and mitigate supply-chain and third-party risks.

Fintech businesses that are reporting issuers (namely, public companies) under Canadian securities legislation are expected and required by the CSA to disclose cybersecurity risks, potential effects of a cybersecurity incident and the governance practices that they have in place to mitigate this type of risk. Registrants (namely, dealers, advisers and investment fund managers) are also expected to be vigilant in keeping their cybersecurity measures up to date, including by following IIROC and Mutual Fund Dealers Association guidance. In general, the CSA expects all regulated entities to adopt a cybersecurity framework recommended by a regulatory authority or standard-setting body that is appropriate for entities of their size. Importantly, IIROC has recently proposed rule amendments that could require mandatory reporting of cybersecurity incidents by investment dealers.

On 9 November 2021, the Office of the Superintendent of Financial Institutions launched a public consultation on the newly released draft version of Guideline B-13: Technology and Cyber Risk Management. The proposed Guideline B-13 is designed to complement existing Guidelines E-21 (Operational Risk Management) and B-10 (Outsourcing of Business Activities, Functions and Processes) as well as the OSFI's Technology and Cyber Incident Reporting Policy, including its Cyber Security Self-Assessment tool.

Read this article on Lexology

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Yes, the Office of the Superintendent of Financial Institutions (OSFI) has issued certain guidelines that would apply to outsourcing by a federally regulated financial services company (such as a bank or insurance company) of a material aspect of its business – specifically, the B-10 Guidelines for Outsourcing of Business Activities, Functions, and Processes (the B-10 Guideline). The B-10 Guideline addresses the OSFI's expectations on federally regulated entities that outsource business activities to service providers, in particular the practices, procedures and standards that should be applied to the outsourcing arrangement. The guideline includes specific guidance for federally regulated entities on due diligence, contractual terms, data location, business continuity, outsourcing in foreign jurisdictions, monitoring and oversight. It also requires that federally regulated entities develop and implement an outsourcing policy. Although the B-10 Guideline does not technically have the force of law, it is nonetheless binding on the regulated entities that are subject to them. Additional regulatory and legislative limits may apply in respect of certain types of financial services companies, such as insurance companies. In April 2022, the OSFI published for comment Draft Revised Guideline B-10 Third Party Risk Management that would replace the existing B-10 Guideline.

Under Canadian privacy laws, organisations generally remain responsible for the appropriate handling of personal information under their custody or control, even where such information has been transferred to domestic or foreign third-party service providers for processing. As such, where a financial services company transfers personal information under its custody or control to a third-party service provider (or that third party collects personal information on behalf of the financial services company) the financial services company must ensure that the information is adequately protected and only collected, used and disclosed in accordance with all applicable Canadian privacy laws. This is typically accomplished through due diligence, robust contractual protections, and periodic audits. Beginning in September 2023, organisations that engage in outsourcing that involves the transfer of personal information to a jurisdiction outside Quebec (including to another Canadian province) will be required by Quebec's Private Sector Privacy Law (RSQ, c 39.1) to first conduct an impact analysis.

Under Companion Policy 31-103, securities registrants must use contractual and other means to provide a comparable level of protection while the information is in the hands of the service provider. Outsourcing organisations are obliged as part of their due diligence to choose vendors with care and, in particular, to ensure that they are contractually bound to comply with appropriate security and confidentiality protocols. Periodic reviews of the service provider, and of the privacy training provided to third-party personnel, are also required in some circumstances.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

The financial services industry must adhere to all applicable Canadian privacy legislation with respect to the use of cloud computing. Federal legislative requirements may, in some cases, require federally regulated financial institutions to maintain certain records in Canada, which can limit the use of cloud computing platforms.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Canada has a robust IP framework. As in any other country, fintech innovations are generally protected through patents, copyrights and trade secrets. Canadian IP databases can be used to search filed or registered trademarks, copyrights and patents.

Inventions that can be patented include products, processes or machines. Computer code in written form has automatic copyright protection. However, if a computer program provides a new solution to a technological problem and modifies how a computer works, the software-implemented invention may be patentable.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

The owner of the invention is entitled to patent it unless there has been an assignment of the invention and the associated IP rights. Express contractual language should be used in employment agreements as best practice to protect IP created by an employee. Barring any specific provision, there is a presumption that employees are entitled to ownership of a patent of any invention they created in the course of their employment. Employers will be deemed owners of the invention and resulting patent rights if there is an express contract stating such and if it can be proven that the employee was employed for the express purpose of inventing or innovating.

In the absence of express terms, the employer is the first owner of the copyright in works that an employee creates in the course of their employment. For contractors or consultants, courts will look at various factors. For work created outside of working hours and (or) using their own resources, the central factor is the subject matter of the copyright work.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Generally, patent co-ownership can be changed by parties through written mutual agreement. However, co-owners of a patent cannot dilute the other co-owners' interests in the patent.

One applicant cannot withdraw a patent application without the consent of the other co-applicants. Similarly, once the patent is registered, one owner cannot license the patent rights to a third party without first obtaining consent from the other co-owners.

For assignment, however, a co-owner may assign his or her own interest in a patent in the absence of the other co-owners' consent unless doing so would dilute the co-owners' rights.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

There is no formal process for protecting a trade secret, or any act or statute that regulates trade secrets in Canada. Trade secret law is developed out of the common law, or in Quebec, civil law, and includes some dispositions in the Criminal Code.

Courts will use several factors to assess whether an action involves the misuse of a trade secret and how to compensate the owner for its misuse. Businesses can also use non-disclosure or confidentiality agreements or clauses and encryption or password protection to protect trade secrets.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brand names and logos can be registered as trademarks for 10 years and renewed indefinitely. Businesses should protect their intellectual property (IP) with registrations and documentation to control ownership and use of their IP rights, including permitted use under licensing and collaborative agreements with third parties.

To ensure that a fintech company is not infringing third-party trademark rights, freedom to operate searches can be conducted to ascertain if there are any prior third-party rights that could pose an obstacle to the use or registration of a mark, or both. Such searches are highly recommended prior to commencing use of a mark as it could become costly to have to transition to a different mark once investments have been made in an original name.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

IP rights holders, not the Canadian Intellectual Property Office, are responsible for enforcing their IP rights. Remedies for infringement include seeking damages sustained as a result of the infringement, the profits made by the infringer, a reasonable royalty and partial court costs or attorney fees. In addition, injunctive relief may be sought as well. In lieu of the above remedies, copyright owners can be compensated through statutory damages (this is a remedy exclusive to copyright infringement claims).

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

There are currently no industry-specific competition or foreign investment issues with respect to fintech companies in Canada. Investments in (and acquisitions of) fintech companies are subject to the same general competition and foreign investment regime as other mergers. However, in recent years, the Canadian Competition Bureau (CCB) has focused its research and advocacy on the importance of innovation and disruption among fintech firms and the potential for this dynamism to be upset by complex regulatory barriers or incumbent market power. In 2017, the CCB published a report titled 'Technology-led innovation in the Canadian financial services sector'. It included recommendations encouraging policymakers to reduce the regulatory barriers to entry associated with fintech products and services and limit the ability of powerful financial incumbents to take steps that frustrate the growth of fintech start-ups.

In December 2022, the federal government tabled legislation to modernise the Investment Canada Act to address 'changing global dynamics' and impose pre-implementation filing requirements for foreign acquisitions of Canadian businesses operating in designated sensitive sectors, which are expected to include, among others, quantum computing and artificial intelligence and companies handling personal data.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

At the federal level, qualifying corporations can claim a tax credit based on eligible scientific research and experimental development (SRED) expenditures. The federal tax credit for Canadian-controlled private corporations (CCPCs) is up to 35 per cent of qualifying

SRED expenditures on a maximum total amount of C$3 million of qualifying SRED expenditures and 15 per cent of qualifying SRED expenditures over C$3 million. However, the C$3 million limit may be reduced if the taxable capital of the CCPC (and associated corporations) exceeds a certain threshold. For non-CCPCs, the federal tax credit is 15 per cent of qualifying SRED expenditures.

For CCPCs, the credit is first applied against federal taxes and the unused portion of the 35 per cent federal tax credit is refundable. A portion of the 15 per cent credit may also be refundable for certain CCPCs. For non-CCPCs, the federal tax credit is not refundable and may only be applied against taxes. In all cases, if the credit is not refundable and cannot be used in a given year, it may be carried forward or carried back to other taxation years in accordance with the detailed rules of the Income Tax Act (Income Tax Act, RSC 1985, c 1 (5th Supp)).

Provinces also offer similar tax credits on research and development expenses, some of which may also be refundable. The provincial credits range from 4.5 per cent to 30 per cent. Certain other industry-specific tax credits are available, depending on the circumstances.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

As of July 2021, new goods and services tax and harmonised sales tax (GST/HST) rules for digital economy businesses came into effect. Non-resident vendors providing cross-border digital services or goods to Canadian consumers as well as platform-based short-term accommodations must register with the Canada Revenue Agency and charge and remit GST/HST if their total taxable supplies are over C$30,000 over a 12-month period. Depending on the provinces, different rates apply.

On 14 December 2021, the federal government released the draft legislation for the Digital Services Tax Act, which will implement a 3 per cent Digital Services Tax (DST). The DST is not expected to apply if a multilateral (OECD) Pillar 1 agreement is reached before 1 January 2024. The DST applies at the rate of 3 per cent on Canadian in-scope revenue in the calendar year generated from digital services (as defined under the Digital Services Tax Act) in excess of C$20 million earned by an individual entity or consolidated group with at least €750 million in global revenue. The earliest any DST will become payable by a taxpayer is mid-2025, but that first payment will be for DST on Canadian digital services revenue earned throughout the 2022–2024 calendar years. In addition, in the 2022 Fall Economic Statement, the federal government affirmed its intention to proceed with the DST and also its intention to implement the OECD's Pillar 1 (reallocation of taxing rights) and Pillar 2 (global minimum tax) approach.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

While there are no specific temporary foreign work programmes tailored to the fintech industry, there are numerous programmes that enable Canadian companies to hire temporary foreign workers in the IT and financial sectors. Canada is also party to a number of multilateral treaties with partnering countries involving the freedom of movement of labour, such as the Canada–United States–Mexico Agreement.

Certain programmes are available for investors and entrepreneurs; however, some programmes may be restricted in terms of the number of participants and be contingent on:

- the province in which the investment will be made;
- the amount of the investment and level of ownership; and
- the provincial agencies that are involved in the establishment of business operations.

One fintech-relevant foreign worker programme, Canada's Global Talent Stream programme (the Program), was implemented by the federal government to help Canadian businesses recruit individuals with technical expertise. The Program's requirements are nuanced but accessible for employers looking to recruit unique and specialised foreign talent to scale up and grow. If a company hires a foreign worker through the programme, it must develop a Labour Market Benefits Plan that demonstrates the company's commitment to activities that will have a tangible and lasting positive impact on the Canadian labour market.

UPDATE AND TRENDS

Current developments

41 Are there any other current developments or emerging trends to note?

Canada's fintech industry continues to flourish, with strong levels of investment and partnerships in both start-up and later stages initiatives. As in other countries, the covid-19 pandemic has accelerated digital transformation, including the shift to digital payments and borderless online trading, fuelled in part by remote work, income support programmes and booming equity markets.

These developments have also accelerated the pace of regulatory developments, both federally and provincially, particularly in the digital payments and crypto spaces.

In October 2020, the Bank of Canada published a report on the foundational principles and core features of central bank digital currencies in conjunction with seven other central banks including the Bank of England and the European Central Bank. The competitive race between central bank digital currencies and privately issued digital currencies globally will

likely accelerate the modernisation and regulation of retail payment systems in Canada. This, in turn, is anticipated to promote the further development of blockchain, cryptocurrency or crypto asset, cloud and other artificial intelligence (AI) technologies. AI is now gaining widespread adoption and is expected to profoundly transform many segments of the financial services industry in Canada. However, the headwinds facing the broader global economy and the tech sector in the post-pandemic high-interest rate and inflationary environment may slow the pace of private funding and create new challenges for the sector in 2023.

* *The information in this chapter is accurate as at December 2022.*

Stikeman Elliott

Alix d'Anglejan-Chatillon	adanglejan@stikeman.com
Ramandeep Grewal	rgrewal@stikeman.com
David Elder	delder@stikeman.com
Shawn Smith	sasmith@stikeman.com
Éric Lévesque	erlevesque@stikeman.com

5300 Commerce Court West, 199 Bay Street, Toronto ON M5L 1B9, Canada
Tel: +1 416 869 5500
www.stikeman.com

Read more from this firm on Lexology

Read this article on Lexology

China

Jingyuan Shi, Yuchen Lai and Yanyu Lai
Simmons & Simmons

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 104
General innovation climate 104
Government and regulatory support 105

FINANCIAL REGULATION 105
Regulatory bodies 105
Regulated activities 106
Consumer lending 107
Secondary market loan trading 107
Collective investment schemes 108
Alternative investment funds 108
Peer-to-peer and marketplace lending 109
Crowdfunding 109
Invoice trading 110
Payment services 110
Open banking 111
Robo-advice 111
Insurance products 112
Credit references 112

CROSS-BORDER REGULATION 113
Passporting 113
Requirement for a local presence 113

SALES AND MARKETING 113
Restrictions 113

CRYPTOASSETS AND TOKENS 114
Distributed ledger technology 114
Cryptoassets 115
Token issuance 116

ARTIFICIAL INTELLIGENCE 116
Artificial intelligence 116

CHANGE OF CONTROL 117
Notification and consent 117

Read this article on Lexology

FINANCIAL CRIME 117
Anti-bribery and anti-money laundering procedures 117
Guidance 118

DATA PROTECTION AND CYBERSECURITY 119
Data protection 119
Cybersecurity 121

OUTSOURCING AND CLOUD COMPUTING 121
Outsourcing 121
Cloud computing 122

INTELLECTUAL PROPERTY RIGHTS 123
IP protection for software 123
IP developed by employees and contractors 123
Joint ownership 124
Trade secrets 124
Branding 125
Remedies for infringement of IP 125

COMPETITION 125
Sector-specific issues 125

TAX 126
Incentives 126
Increased tax burden 126

IMMIGRATION 126
Sector-specific schemes 126

UPDATE AND TRENDS 127
Current developments 127

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

China's reputation as a global leader in fintech innovation continues to grow, and fintech companies in China have particular expertise in areas such as payments, artificial intelligence (AI), blockchain and digital currency. Going forward, we expect fintech innovation in China to play a substantial role in the development of the entire financial services industry. The Chinese government actively encourages innovation by fintech companies. However, the fintech sector remains highly regulated and this seems unlikely to change. In fact, it is possible that fintech companies may be subject to greater regulatory supervision in the future, especially where they carry out business related to online insurance, the centralised storage of deposits in payments sectors, AI, cybersecurity and data protection.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

In January 2022, the People's Bank of China (PBOC) issued the Fintech Development Plan (2022–2025) (the Fintech Plan), which highlights the importance of financial innovation via fintech development. The Fintech Plan outlines the basic principles, including digital drive, AI, green and low carbon emission, fairness and inclusiveness. The Fintech Plan also sets the development goals, including digital transformation in the financial industry, full use of data resources, improved financial service quality and efficiency, mature governance system for the fintech industry, use of core tech applications and more advanced digital infrastructure. The Fintech Plan also sets out a total of 28 major tasks covering eight areas, including measures to strengthen data capabilities, orderly sharing of data, comprehensive use of data, data security, etc.

The Fintech Plan represents the digital direction of fintech development in China for the four-year period. Considering that China has put in place major data laws such as the Data Security Law and the Personal Information Protection Law, both of which took effect in late 2021, fintech innovation balanced with data law compliance will be the new focus for the digital transformation of financial services and fintech regulatory framework in the near future.

Sandbox schemes have been introduced and expanded to 29 provinces and cities since December 2019. Until the end of April 2022, over 150 fintech applications had been covered by the sandbox schemes. Until May 2023, several provinces and cities including Beijing, Shanghai and Shenzhen have released a number of projects coming 'out of the boxes' and entering into pilot operations.

The relevant provinces and cities have also issued their own incentive plans. A recent example is Shenzhen, where the local government announced in April 2022 that financial subsidies and other favourable policies will be granted for innovative fintech projects. The city also pledges to improve relevant public services for the fintech sector. Likewise, Beijing announced in June 2022 to provide full-chain financial support for fintech innovation enterprises, such as credit risk compensation and capital subsidies for listing.

In addition, fintech companies may apply for various tax incentives for high-tech companies and free trade zones, where eligible.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

There is no single regulatory body responsible for the regulation of fintech products and services. Different fintech services and products are regulated by different regulatory bodies. The main regulatory bodies include the People's Bank of China (PBOC), China Securities

Regulatory Commission (CSRC) and State Administration for Financial Regulation (SAFR), which replaced the former China Banking and Insurance Regulatory Commission (CBIRC) on 18 May 2023.

The regulators' authorities are also adjusted following the restructuring. The SAFR is responsible for the regulation of all financial sectors except the securities sector, financial consumer protection, and investor protection (which used to be within the authorities of the CSRC). The CSRC is now responsible for the regulation of capital markets, including the approval of issuance of corporate bonds (which used to be within the authorities of China's National Development and Reform Commission). The PBOC continues to be responsible for formulating and executing currency policies.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

The following activities are regulated and require a financial licence:

- carrying on securities brokerage;
- carrying on securities investment consultancy;
- financial advising relating to securities trading or investment;
- securities underwriting and sponsorship;
- carrying on proprietary account transactions;
- carrying on securities asset management;
- taking in deposits from the general public;
- handling domestic and foreign settlements;
- handling, accepting and discounting of negotiable instruments;
- issuing financial bonds;
- acting as an agent for the issue, honouring and underwriting of government bonds;
- buying and selling government bonds and financial bonds;
- offering and providing discretionary investment management services;
- buying and selling foreign exchange, and acting as an agent for the purchase and sale of foreign exchange;
- operating insurance companies;
- operating insurance agencies and insurance intermediaries;
- carrying on fund management services;
- carrying on fund custodian services;
- carrying on derivative products transactions;
- lending microloans online or offline;
- providing consumer financial services;
- providing third-party payment services;
- providing financial lease services;
- providing financing guarantee services;
- carrying on futures trading services;
- providing credit services;
- providing commercial factoring services;
- operating financial holding companies; and
- operating trust companies.

Read this article on Lexology

Note that pawn broking is also related in China, under the supervision of the Ministry of Commerce (instead of financial regulators).

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Consumer lending is a regulated activity and is governed by the General Rules of Loans, the Administrative Measures for Pilot Consumer Finance Companies (the Consumer Finance Measures) and the Commercial Bank Law. The former CBIRC also issued the Trial Rules for Supervision Rating for Consumer Finance Companies (Trial Rating Rules).

According to the General Rules of Loans, to engage in the lending business, lenders must be approved by the PBOC to hold a financial institute legal person permit or a financial institute operation permit issued by the PBOC, and they must be approved and registered by the State Administration for Market Regulation.

The Consumer Finance Measures regulates the operating activities of consumer finance companies that refer to non-bank financial institutions and do not receive public deposits but provide loans to resident individuals within China for consumption purposes (excluding house and vehicle purchases) under the principle of small sum and dispersion. The consumer finance companies used to be approved by the former CBIRC.

Under the Trial Rating Rules, the former CBIRC will provide rating results to consumer finance companies. Such companies will be subject to different regulatory measures according to their rating results.

The former CBIRC's responsibilities shall be assumed by the SAFR.

Secondary market loan trading

6 | Are there restrictions on trading loans in the secondary market in your jurisdiction?

Trading loans between financial institutions in the secondary market are subject to regulatory supervision by the SAFR (formerly the CBIRC) and the following restrictions:

- the financial institutions must report certain information to the SAFR (formerly the CBIRC);
- the transfer of loans is subject to the consent of the borrower and the guarantor (if any);
- all outstanding principal and interest must be transferred as a whole;
- parties are prohibited from making any direct or indirect repurchase arrangements; and
- if the lender is from a consortium, other members of the consortium shall have the right of first refusal for such a transfer.

Trading loans between non-financial institutions are generally not subject to mandatory regulatory restrictions.

On 7 January 2021, the former CBIRC published a notice on Implementing the Pilot Program of Transferring Non-performing Loans. Selected state-controlled or joint-stock banks participated in the pilot programme. Only individual corporate non-performing loans and batch personal non-performing loans are included in the pilot programme. According to public records from the registration centre of intrabank credit assets, qualified banks are quite active in trading non-performing loans. A single listing from Ping An Bank worth 1.14 billion yuan was successfully transferred in September 2021.

On 30 December 2022, the former CBIRC announced to carry out the second phase of the pilot programme, to include more state-owned banks, as well as trust companies, consumer finance companies, automotive finance companies, financial leasing companies, and urban commercial banks and rural small and medium-sized banking institutions registered in 11 provinces and cities.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

'Collective investment scheme' is not defined under Chinese law. The establishment and operation of securities investment funds within China via the public and non-public raising of funds is regulated by the Securities Investment Fund Law. The primary regulatory body for funds in China is the CSRC. Generally, the regulation on public raising funds (retail funds) is more detailed and restrictive than for private funds. Retail funds and retail fund managers must be registered with the CSRC. Fundraising, fund custodian and investment activities are strictly regulated by the CSRC. Agencies that engage in sales, sales payment, unit registration, valuation services, investment consulting, rating, information technology system services and other fund services related to publicly raised funds are subject to registration or record-filing in accordance with the requirements of the CSRC. Private funds and private fund managers must register with the Asset Management Association of China, an industry self-disciplinary body under the supervision of the CSRC.

Pursuant to article 2 of the Securities Investment Fund Law, the definition of 'securities investment funds' is funds managed by fund managers, placed in the custody of fund custodians and used in the interest of the holders of the fund units for investment in securities. Accordingly, peer-to-peer or marketplace lenders or crowdfunding platforms do not fit the definition of collective investment schemes and do not fall into the regulatory scope of the Securities Investment Fund Law.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Managers of alternative investment funds that raise capital from a number of investors and invest it in accordance with a defined investment policy for the benefit of those investors are regulated. These activities are broadly defined as asset management services, and may be conducted by securities companies, trust companies and fund management companies and

their subsidiaries. Managers are subject to different regulatory regimes depending on the specific form of these alternative investment funds.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

The Interim Measures for the Administration of Business Activities on Online Lending Information Intermediary Agencies (the Online Lending Rules), issued on 17 August 2016 by the former CBIRC, specifically target the activities of peer-to-peer lending between individuals through an internet-based platform. The Online Lending Rules require that the peer-to-peer lending platforms register with the local financial regulatory offices, apply for the applicable telecommunication service operation licence and include serving as an internet lending information intermediary in its business scope, and shall only act as information intermediaries between parties. Peer-to-peer lending platforms must not conduct credit enhancement services, cash concentration or fundraising activities for themselves, or provide security or guarantee arrangements for lenders. The Online Lending Rules also set out detailed requirements for information disclosure, protection of lenders and borrowers and risk control measures.

In the years 2017 to 2019, the Chinese government and relevant regulatory authorities issued various regulations and guidelines governing the peer-to-peer online lending industry. The main purpose was to regulate peer-to-peer industry behaviour and enhance supervision of the industry. However, peer-to-peer online lending in China is often linked with illegal fundraising, which has caused significant economic losses to investors and massive social unrest in many places. A majority of the local provinces in China took measures to effectively prohibit its operation. According to the PBOC, existing peer-to-peer online lending institutions had all suspended operations in the country by April 2020. The former CBIRC revealed in March 2022 that 490 billion yuan of peer-to-peer loans had not been redeemed. So far, there is no sign of reopening of peer-to-peer online lending operations.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

The Guideline Opinion on Promoting the Healthy Development of Internet Finance has defined equity-based crowdfunding as public equity financing in small amounts through an internet-based platform. The Opinion provides that equity crowdfunding must be conducted through an agency platform such as a website or other digital medium and that the CSRC will be the regulatory authority for equity crowdfunding business. In 2016, the CSRC issued an action plan for risk control of equity-based crowdfunding, prohibiting the establishment of private equity funds or a public offering of securities through crowdfunding.

However, in practice, crowdfunding is often abused by operators to illegally raise capital, which has led to waves of government crackdowns. Crowdfunding is increasingly having a negative impact and therefore not welcomed by the regulators.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

The Negotiable Instruments Law, issued in 2004, applies to three categories of negotiable instruments including money orders, promissory notes and cheques. It provides rules for the transfer, endorsement, acceptance and payment of the three negotiable instruments.

Account receivables can be used for financing purposes in China. Such financing is particularly encouraged under the Law on Promotion of Small and Medium Enterprises, but currently, there is no specific law or regulation on the matter. The CSRC and the PBOC jointly issued the Guiding Opinion on Promotion of the Sound Development of Chattel and Title Financing, under which the regulators expressly require banking institutions to expand the scope of guarantees to include unpaid and overdue invoices. The regulators also encourage banks to use blockchain technology to facilitate invoice trading and to develop online invoice trading products to satisfy the needs of SMEs. The Credit Reference Centre of the PBOC operates an online platform to register account receivables, which are used to obtain financing funds from banks, qualified non-bank financial institutions or factoring companies.

Payment services

12 | Are payment services regulated in your jurisdiction?

Payment services provided by non-financial institutions (payment services providers) in China are primarily regulated by the PBOC under the Administrative Measures for the Payment Services Provided by Non-financial Institutions (Payment Measures). Payment services refer to any of the following transfer services provided by non-financial institutions as the intermediaries between the payer and the payee:

- online payments;
- issuance and handling of prepaid cards;
- bank card acquiring; and
- any other payment services as determined by the PBOC.

A payment service provider is required to obtain a payment service licence issued by the PBOC to provide payment services in China. For cross-border payments in foreign currencies, payment services providers will need to obtain an approval from the foreign exchange authority (ie, the State Administration of Foreign Exchange (SAFE)), in addition to the payment licence issued by the PBOC. The PBOC issued the Notice on Matters Relating to Foreign Invested Payment Institutions in 2018, clarifying that where an overseas institution intends to provide electronic payment service to the domestic transactions and cross-border transactions of China-based customers, it shall set up a foreign-invested company within China and apply for the payment service licence in accordance with the Payment Measures. However, it is worth noting that the PBOC has not granted any new payment service licence since 2015. As of 6 June 2023, PayPal and Airwallex are the only two overseas institutions that have obtained licences for online payment by acquiring existing licence holders.

According to the Measures for the Deposit of Pending Payments of Clients of Non-bank Payment Institutions issued by the PBOC in January 2021, non-financial payment institutions must deposit customer reserve funds in accounts with the PBOC or qualified commercial banks to protect the funds.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

There are currently no such laws or regulations in China. On 13 February 2020, the PBOC issued the financial industry standard of the application programming interface secure management specification for commercial banks (not mandatory but recommended). The standard specifies the type and security level of the application programming interface (API) of commercial banks and the security design, deployment, integration, operation and maintenance, termination and system downline and management, as well as other security technology and requirements.

Further, according to the Fintech Plan (2022–2025) published by the PBOC, China will continue to promote the upgrading of digital channels (such as API) and establish 'comprehensive financial service platforms'. The Fintech Plan also states that multiple technologies will be used in exploring secure data sharing; data sharing and ownership determination mechanisms will be explored as well. The goal is to achieve cross-institution, cross-region and cross-industry data sharing in an orderly fashion. Therefore, it is expected that China will implement trial programmes to promote data sharing by financial institutions in the near future.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

In 2018, the PBOC, the former CBIRC, the CSRC and SAFE jointly issued the Guidelines on Standardising the Asset Management Business of Financial Institutions (the Guidelines). The Guidelines define robo-advice as a form of artificial intelligence in offering investment consulting services, and, thus, institutions or personnel carrying out robo-advice services must obtain relevant investment consulting service qualifications. The Guidelines confirm that robo-advice services must also strictly comply with the general rules of asset management services, such as the rules regarding the suitability of investors, investment scope, information disclosure and risk isolation. In addition, the Guidelines also highlight that the development of investment algorithms must be diverse, thus avoiding the increase of the pro-periodicity of investment behaviour.

In addition, some cities, such as Shanghai and Beijing, have issued incentive plans for new businesses that include robo-advisors. For example, Shanghai has issued the Action Plan for Promoting the Development of Online New Businesses of Shanghai City.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Yes. In addition to the general insurance laws and regulations, internet insurance companies are obliged to comply with the Measures for the Regulation of Internet Insurance Business issued by the former CBIRC. Insurance companies and brokers must be licensed to carry out their business. They are permitted to conduct internet insurance business on their own online platforms or through third-party online platforms.

In October 2021, the former CBIRC issued the Notice on Further Regulating Internet-based Life Insurance Business of Insurance Companies, which provides conditions and restrictions for insurance companies to operate life insurance businesses online.

China's financial, foreign exchange, telecom, cyberspace and IP regulators jointly issued the draft Administrative Measures on Online Sales and Marketing of Financial Products in January 2022. These draft measures further clarify that licensed financial institutions may entrust internet platform operators to conduct sales and marketing of financial products, while the internet platform operators must not get involved in regulated activities, unless otherwise approved. The regulated activities spelt out include providing interactive consulting services to consumers, conducting suitability assessments of financial consumers, entering into sales agreements, handling funds transfers, etc.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Yes. The Administrative Regulations on the Credit Reporting Industry and the Administrative Measures on the Credit Reporting Business are the primary regulations for credit references and credit information services. The providers of credit rating services and corporate credit information services are subject to filing requirements with the PBOC, while the providers of personal credit information services are subject to prior approval from the PBOC and stricter qualification requirements. Financial institutions are prohibited from obtaining credit services from market players without relevant qualifications.

In addition to general personal data protection principles, personal credit information service providers are subject to specific notification obligations. They are required to notify the PBOC of their plans for the collection and use of personal data, including the types and sources of data, manners of collection, the mechanism for privacy rights protection and data processing vendors.

As of 6 June 2023, over 130 corporate credit information services providers have completed the filing with the PBOC, while only two companies are granted approval to carry out personal credit information services.

In December 2022, China's National Development and Reform Commission published the draft Law on the Construction of Social Credit System for public consultation. The draft law

contains a standalone chapter on the supervision of credit business, proposing that the state will apply unified approval management of credit business. It is unclear when the draft law will be submitted to the National People's Congress.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

Regulated activities cannot be passported into China.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

In our experience, a licence for regulated activities would only be granted to an entity that has a local presence. Therefore, it is unlikely that Chinese regulators, including the People's Bank of China, China Securities Regulatory Commission (CSRC) and State Administration for Financial Regulation, would grant a licence for regulated activities to an entity that was not permanently established in China. Under special circumstances, foreign securities companies may conduct certain activities within China subject to the approval of the CSRC. Foreign institutions may provide financial information services without a local presence in China subject to the approval of the Cyberspace Administration of China, which is the primary authority for internet content regulation in China.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

The sale of financial services and products is regulated by different regulatory bodies depending on the type of financial services and products being sold. For example, the sale of fund products is subject to the approval of the China Securities Regulatory Commission and the sale of insurance products is subject to the approval of the State Administration for Financial Regulation, formerly the China Banking and Insurance Regulatory Commission.

Regarding the marketing of financial services and products, different requirements are applicable to different types of services.

In relation to securities-related services, for example, securities companies are required to obtain sufficient knowledge of the investors and recommend suitable products and services based on the situation of each investor. Securities companies must ensure that investors understand the risks clearly and each investor must sign a risk disclosure statement.

Securities companies are not allowed to promise guaranteed profits to the investors or make up for losses in promoting or marketing financial products.

For insurance services, internet insurance institutions must not make any misrepresentations, exaggerate previous track records or promise guaranteed profits as part of the marketing process. Information concerning insurance products, services, premiums, etc, must be clearly presented to the customers.

China is also in the process of formulating a new regulation on the online sales and marketing of financial products. The draft regulation published in January 2022 (still pending finalisation) sets out different obligations for licenced financial institutions (as the providers of financial products) and third-party internet platforms. This draft regulation also provides specific codes of conduct for online marketing activities, such as targeted marketing, webcasting, anti-spam, etc, as well as data and intellectual property protection issues.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

On 10 January 2019, the Cyberspace Administration of China (CAC) issued the Administrative Provisions on Blockchain Information Services (the Blockchain Provisions), which came into effect on 15 February 2019. The Blockchain Provisions apply to blockchain information services in China, which are defined as information services delivered to the public by way of the internet or computer application programs based on blockchain technology or systems. The Blockchain Provisions do not require blockchain service providers to obtain special operating permits from regulators. However, if the blockchain services fall within the application scope of other Chinese rules, such as telecom business-related regulations, the blockchain service will still be subject to operating permits under those rules. Although there is no operating permit requirement for providing blockchain services, the Blockchain Provisions require blockchain service providers to file a record with the CAC within 10 working days from the commencement of the blockchain services. In addition, the Blockchain Provisions set out certain security requirements for blockchain service providers. For example, blockchain service providers should certify the real identity of blockchain service users by checking relevant information and keeping the login records of the users for at least six months.

In October 2019, the Central Committee of the Communist Party of China organised a special study on blockchain technology chaired by Chinese President Xi Jinping, who promoted the use of the technology and its industrial innovation and development. This top-level endorsement was viewed as an encouragement to those in the sector, which has been dampened since the ban on initial coin offerings (ICOs) in 2017 (however, there has been no relaxation of this ban).

On 5 February 2020, the People's Bank of China (PBOC) published an industry standard regarding Financial Distributed Ledger Technology Security Specification.

Read this article on Lexology

In the Fintech Development Plan (2022–2025) issued by the PBOC, the regulator proposes to fully utilise blockchain technology and use distributed ledger, smart contract and consensus mechanisms to address the issues of data security, integrity and trustworthiness of internet-based transactions and provide support for supply chain finance and trade finance, etc.

In March 2023, the Ministry of Industry and Information Technology issued a draft guidance for public consultation, regarding the national standards to be formulated for the development, application and security protection for blockchain and distributed ledger technology.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

The PBOC, together with six ministries, issued the Notice on Preventing Financial Risks relating to Initial Coin Offerings on 7 September 2017, which remains the primary regulation on ICOs. The Notice states that all financial institutions and non-banking payment institutions in China must not directly or indirectly provide products or services for ICO financing and cryptocurrency activities, including account opening, registration, trading, clearing and settlement services, and must not provide insurance services for ICOs and cryptocurrency activities or include any of them in insurance coverage.

On 15 September 2021, the PBOC, together with seven ministries, the Supreme People's Court and the Supreme People's Procuratorate, issued the Notice on Further Prevention and Disposal of the Risk of Speculation in Virtual Currency Trading (the Virtual Currency Notice). The Virtual Currency Notice provides a series of stringent rules against the crypto business, including but not limited to:

- Bitcoin, ether and tether are all deemed as 'virtual currencies'. Business activities in relation to these virtual currencies are all 'strictly prohibited', including exchange between fiat money and virtual currencies or among different virtual currencies, trading virtual currencies as a central counterparty, providing infomediary or pricing services for virtual currencies, ICO and derivative trading.
- Overseas exchanges providing services via the internet to Chinese residents are deemed as an illegal financial activity. The China-based staff of the overseas exchanges, as well as the organisations and individuals who knowingly provide marketing, sales, payment clearance and technical support to the overseas exchanges will be held liable for non-compliance.
- Internet companies are prohibited from providing online operational space, commercial display, marketing, sales or paid traffic direction services for virtual currency-related activities. Cyberspace and telecom regulators will take actions to shut down websites, mobile applications and mini-apps that conduct virtual currency-related activities.
- The PBOC and the CAC will intensify technical monitoring of mining, transactions and exchange of virtual currencies.

In light of the above, virtual currency is generally not recognised and virtual currency issuance and trading are prohibited in China.

Read this article on Lexology

The PBOC initiated its Digital Currency Electronic Payment (DCEP) project study back in 2014. The DCEP is the digital version of the renminbi and has the same legal status and functionality as paper currency. The value of DCEP is also backed by state credit. The DCEP will be distributed to the market through the PBOC and other commercial banks and banking institutions. In April 2020, China became the first major world economy to test digital currency. According to official statistics, the tests have been launched in 17 Chinese provinces as of April 2023 and DCEP in circulation has exceeded 13.6 billion yuan by the end of 2022.

However, the DCEP is fiat money, and its development does not in any way suggest a change in the regulator's attitude towards cryptocurrencies.

There are currently no laws or regulations specifically governing NFTs in China. Several NFT-related companies have successfully filed as blockchain service providers to carry out their businesses. In April 2022, the National Internet Finance Association of China, China Banking Association and Securities Association of China jointly launched an initiative on preventing NFT-related financial risks, in which they require their members not to issue financial products or conduct ICOs in the disguised form of NTFs, not to establish a market-place for NTF trading in violation of regulations, not to use virtual currencies in NFT pricing or settling, not to directly or indirectly invest in NFTs or provide financing support for NFT investment, and to verify the true identities of NFT issuers, sellers and buyers and perform AML obligations.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Virtual currency trading is prohibited in China, and digital currency exchanges and brokerages are also banned.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

In 2018, the People's Bank of China, the China Banking and Insurance Regulatory Commission, the China Securities Regulatory Commission and the State Administration of Foreign Exchange jointly issued the Guidelines on Standardising the Asset Management Business of Financial Institutions (the Guidelines). The Guidelines define robo-advice as an investment consulting service, and, thus, institutions or personnel carrying out robo-advice services must obtain relevant investment consulting service qualifications. The Guidelines confirm that robo-advice services must also strictly comply with the general rules of asset management services, such as the rules regarding the suitability of investors, investment scope, information disclosure and risk isolation. In addition, the Guidelines also highlight

that the development of investment algorithms must be diverse, thus avoiding the increase of the pro-periodicity of investment behaviour.

The Administrative Provisions on Algorithmic Recommendations for Internet Information Services issued by the Cyberspace Administration of China, effective on 1 March 2022 (the Algorithm Rule), applies to online services deploying recommendation algorithms within China, which may include, without limitation to, personalised pushing, sequence refinement, search filtering, etc. Internet information service providers (including certain fintech companies) are required to inform users in a conspicuous way if algorithms are being used to push content to them and to disclose the basic principles, purposes and mechanics of their algorithm-recommended services. Internet information service providers are not allowed to use algorithm-recommendation services to induce overconsumption, facilitate monopoly or unfair competition.

According to the 2023 legislation plan of China's State Council, as published in June 2023, the draft Law on Artificial Intelligence is anticipated to be submitted to the National People's Congress for deliberation within this year.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

In general, if a regulated business changes control it must make a change of registration application to the regulatory authority. The change of control may only take place after the change of registration has been approved.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Yes. The Administrative Measures for Anti-money Laundering and Counter-terrorism Financing by Internet Finance Service Agencies (for Trial Implementation) issued by the People's Bank of China (PBOC) and the former China Banking and Insurance Regulatory Commission, effective on 1 January 2019, applies to all the approved institutions that carry out internet finance business in China. Internet finance businesses include but are not limited to online payment, internet lending, internet lending information intermediary services, equity crowdfunding financing, internet fund sale, internet insurance, internet trust and internet consumption finance.

Additionally, the Measures for the Supervision and Administration of Combating Money Laundering and Financing of Terrorism by Financial Institutions issued by the PBOC, effective

on 1 August 2021, also applies to certain fintech companies, such as internet microfinance companies. Internal control and risk management systems shall be established accordingly. The PBOC or its branches may carry out onsite reviews or investigations.

Institutions other than financial institutions and non-banking payment institutions must register the fulfilment of duties in anti-money laundering and counter-terrorism financing on the online monitoring platform set up by the PBOC, while financial institutions and non-banking payment institutions may, depending on the need for anti-money laundering work, connect with the online monitoring platform to participate in the exchange of work information, share technical facilities and assess risks.

Other major requirements for institutions carrying out internet finance business include, among others:

- establishing an internal control system and compliance management policies for anti-money laundering and counter-terrorism financing and reporting these systems and policies to relevant regulators;
- conducting know-your-client (KYC) checks with due diligence;
- putting in place a monitoring and reporting system for large amount transactions and doubtful transactions; and
- cooperating with on-site and off-site inspections and anti-money laundering investigations conducted by the PBOC or its local branches.

In addition, under regulations for third-party payment transactions, KYC checks must be completed on clients for anti-money laundering purposes and there are annual limits on outgoing payments. Payment platform operators can offer three types of accounts that have escalating regulatory requirements. Accounts with lower annual limits have lower minimum KYC requirements and accounts with higher annual limits have more comprehensive KYC requirements.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

Yes. On 6 February 2017, Minutes of the Symposiums of the Supreme People's Procuratorate on Issues Concerning Handling Internet-related Financial Crime Cases was published. Although the minutes do not have any legal effect, they represent the enforcement trends and focuses in relation to financial crime for fintech companies. The scope and boundary of prosecution and explanation of the definitions of several high-profile crimes were discussed.

Courts and procuratorates at various levels also publish model cases of financial crime from time to time, to raise the awareness of the general public.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The key regulations governing the processing and transfer of data are the Chinese Cybersecurity Law, the Data Security Law and the Personal Information Protection Law (PIPL).

The Cybersecurity Law became effective in 2017. It sets out the main requirements and principles related to cybersecurity and data privacy. The Cybersecurity Law is not specifically aimed at fintech companies. Instead, it applies generally to a 'network operator', which is broadly defined as 'the owner or manager of a network, or a network service provider'.

The Data Security Law became effective on 1 September 2021. It addresses all data processing activities and relevant safety supervision within China. According to the Data Security Law, innovative use of data is encouraged, a data security standard system will be constructed, a data security check and assessment and certification will be promoted and a data trading system will be established. Further, according to the Data Security Law, a multi-layered data protection classification system will be established. Catalogues of 'important data' will be formulated and published by regional and sectoral regulators.

The PIPL became effective on 1 November 2021. The law has extraterritorial effect – that is, it applies not only to data processing activities within China, irrespective of the location or nationality of data subjects, but also to the offshore processing of personal data of China-based individuals, if the purpose of such processing is for offering products or services to such China-based individuals or analysing or assessing their behaviours. The PIPL provides more legal bases for data processing besides consent, including, among others, the necessity to conclude or perform the contract to which the data subject is a party and the necessity to perform legal duties or legal obligations.

Pursuant to the Cybersecurity Law and the PIPL, data processors (equivalent to data controllers in the GDPR context) may transfer data out of China following different routes, depending on the nature of the data processor and the volume of the personal data involved. Two long-awaited implementation regulations are issued by the Cyberspace Administration of China (CAC) in mid-2022 and early 2023, setting out detailed provisions on the security assessment for data export (Security Assessment) and the standard contract for personal data outbound transfer (Standard Contract).

The Regulation on Security Assessment for Data Export (the Security Assessment Regulation) provides that the following situations will be subject to the Security Assessment requirement:

- any data exporter to transfer 'important data' out of China;
- any critical information infrastructure operator to transfer personal data out of China
- any personal data processor that processes the personal data of more than 1 million individuals to transfer personal data out of China; and

- any personal data processor that has transferred the personal data of 100,000 individuals or the sensitive personal data of 10,000 individuals out of China since 1 January of the previous year to transfer personal data out of China.

The Security Assessment is in essence a process of administrative approval. In practice, the CAC applies very high standards when reviewing the application documents. Fintech companies with retail businesses are likely to trigger this obligation, given their client base and the sensitive personal data involved (note that financial account information is deemed as sensitive personal data under Chinese law).

If the Security Assessment thresholds are not triggered, the data exporter may transfer personal data out of China by following the Regulation on the Standard Contract for Personal Information Outbound Transfer and entering into the standard contract with the overseas recipient (China SCCs). The China SCCs share a fair amount of similarities with the EU's Standard Contractual Clauses for international data transfer while maintaining significant unique features.

In addition to the above laws and regulations that apply to all sectors, there are other measures, industrial-specific rules and non-mandatory specifications governing the processing and transfer of data relating to fintech products and services.

For example, the Implementation Measures on the Protection of Rights and Interests of Financial Consumers as effective on 1 November 2020, sets out a standalone chapter on the protection of consumer financial information. Financial institutions are required to notify the relevant local branches of the People's Bank of China (PBOC) immediately, if an information breach incident may harm the personal and property security of consumers, or within 72 hours, if the breach incident may have other adverse impacts on consumers.

Credit businesses must not collect sensitive personal data relating to, for example, religion, gene information, fingerprints, blood type, diseases and other medical history, or other information prohibited by law. They are required to process and store the data collected in China locally and follow relevant rules set out by law when conducting cross-border transfers.

Insurance companies are required to store 'important data' such as operational and financial data within China, with independent storage facilities, appropriate security safeguards and offsite backup measures.

Besides the mandatory laws and regulations, several national and industrial standards are also notable to fintech companies, such as the Personal Financial Information Protection Technology Specification issued by the PBOC. This specification classifies personal financial data into three categories according to the level of sensitivity and requires personal financial data to be transferred via safe channels or in the form of encrypted data.

The Guide for De-identifying Personal Data and the Guide for Evaluating the Effectiveness of Personal Data De-identification (both are recommendatory national standards) provide guidance on the de-identification of personal data.

Read this article on Lexology

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

There are no cybersecurity regulations specific to fintech business. The general cybersecurity obligations of network operators under the Cybersecurity Law include requirements to:

- establish internal cybersecurity policies and procedures;
- implement proper technical measures to prevent hacking and viruses as well as to monitor network operations;
- retain network operation records and logs for at least six months;
- formulate and implement contingency plans;
- address cyber risks known to the operators; and
- report any cybersecurity incident to the government and the customers affected by the incident.

In September 2022, the Cyberspace Administration of China published the draft amendment to the Cybersecurity Law for public consultation. Though obligations of the network operators remain unchanged, much heavier penalties are proposed for violations of the law, with the maximum fine increasing from 1 million yuan to 50 million yuan or 5 per cent of the network operator's annual turnover of the previous year.

Several industrial standards published by the PBOC cover specific cybersecurity issues of financial institutions, such as disaster recovery, data centre management, the infrastructure of non-banking payment agencies, cloud computing applications, etc. Three standards published in October 2020 are in particular closely related to fintech businesses:

- the General Security Specification for Fintech Innovation;
- the Application Testing Specification for Fintech Innovation; and
- the Risk Monitoring Specification for Fintech Innovation.

Financial institutions are encouraged to use the industrial standards as practical guidance, though they are not mandatory.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

The former China Banking and Insurance Regulatory Commission issued the Guidelines of Risk Management for Outsourcing by Banking Financial Institutions on 4 June 2010. The Guidelines define outsourcing activities as entrusting service providers to continually process certain business for and on behalf of the banking institutions themselves. The board of directors and senior management of the banking institutions shall be ultimately responsible for the outsourcing activities. The banking institutions must conduct a risk

assessment prior to engaging any outsourcing service providers. The banking institutions must enter into written agreements with service providers and establish a client information confidentiality mechanism. Additionally, the service providers must not subcontract any outsourcing business to third parties.

On 30 December 2021, the former CBIRC issued the Measures for the Regulation of Risks in Information Technology Outsourcing by Banking and Insurance Institutions, which provide more detailed requirements on outsourcing in terms of risk evaluation, due diligence, contracting, security management, supervision and assessment, important outsourcing and risk events reporting, and services suspension and termination. The outsourcing providers may only subcontract non-material parts of their services.

In accordance with the Provisions on Administration of Filing of Securities Service Institutions Engaging in Securities Services as effective on 24 August 2020, qualified securities service institutions shall be filed with China Securities Regulatory Commission (CSRC) to provide certain securities services, including accounting firms, law firms and institutions engaging in asset appraisal, credit rating, financial advisory or information technology system services. As of 31 March 2023, 379 information technology system service institutions have been announced by CSRC to complete the filing.

The Asset Management Association of China (AMAC) issued the Interim Administrative Measures for Private Funds Services Business on 1 March 2017. The Measures require that service providers providing fundraising, investment consulting, fund unit registration, valuation and audit and information technology system services to private fund managers register with the AMAC. The service providers must not subcontract any such outsourcing business to third parties.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

Cloud computing is deemed a type of value-added telecommunication service and requires a telecoms service licence. There are no specific legal rules relating to the use of cloud computing in the financial sector, but the State Council has issued several related policy documents, such as the Guiding Opinions on Actively Promoting the 'Internet Plus' Action Plan (2015) and the Opinions on Promoting the Innovation and Development of Cloud Computing and Fostering New Business models of Information Industry (2015), where the use of cloud computing in the financial sector and the use of online financial cloud service platforms are encouraged.

As for the choice of public, private or hybrid cloud solutions, deployment of public cloud by financial institutions (or companies in other sectors) is not straight out prohibited by existing laws or regulations. However, the financial sector is heavily regulated and financial institutions are subject to various legal requirements regarding their IT infrastructure and information system deployment. Such requirements are scattered in different sectoral rules and standards, with meticulous technical requirements in relation to the supervision of data centres, information system security protection, disaster recovery, IT outsourcing, etc. Such vigorous IT requirements mean that financial institutions have to choose a cloud service

that offers a higher standard of security, stability and resilience than many public clouds can offer. Therefore, financial institutions are driven towards private and hybrid cloud solutions.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Computer software is protected by copyright as an independent category of work. The subject of copyright is the code script of the software and not the operating process or results of the software.

Software copyright arises automatically upon completion of the code script. Although registration is not a mandatory requirement for granting copyright, there is a specific procedure for software copyright registration under Chinese law. Copyright issuers may apply to the China Copyright Protection Centre for the registration of software copyright, licence agreement and assignment agreement of the software copyright.

If the software code has been kept confidential it may also be protected as confidential information. No registration is required.

Although it is not common, software can also be protected by patents as long as the software demonstrates novelty, creativity and applicability as required by patent laws. Patents must be applied for, granted and registered before the competent patent office.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

The copyright of works created mainly by using the materials and technical resources of the employer (and that were the employer's responsibility) shall belong to the employer. Otherwise, any work created during the course of employment shall belong to the employee who develops it. However, the employer has the priority right to exploit the work within the scope of its normal business operation. Further, the author may not authorise a third party to use the work in the same manner in which his or her employer uses it, without the employer's consent, within two years of the work's completion.

The patent right of an invention accomplished in the course of performing normal employee duties or mainly by using the material and technical resources of the employer shall be owned by the employer.

However, in practice, most employers, especially technology companies, will specify in the employment contract that all intellectual property rights of works and inventions developed

during the course of employment or for the purpose of fulfilling a work assignment are owned by the employer.

The rules do not apply to new intellectual property developed by contractors or consultants unless otherwise agreed, the intellectual property rights of inventions or works developed by contractors or consultants shall be owned by the contractors or consultants.

In practice, it is often provided in the commissioning contract that the commissioner owns the intellectual property rights of the work, or that the author owns the rights but shall grant the commissioner an exclusive and royalty-free licence to use the commissioned work for the purposes contemplated at the time of the commissioning.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

The joint owners of intellectual property rights must negotiate and reach agreement on the use, licensing and assignment of these intellectual property rights. If no such agreement exists, any joint owner has the right to use or grant a non-exclusive licence to third parties, and the licence fees collected shall be distributed among all joint owners. The granting of a sole or exclusive licence, and the charge, assignment or other disposal of the intellectual property rights shall be subject to the consent of all joint owners.

The joint owners of a trademark are not subject to the above restrictions. This is because, usually, the joint owners register the trademark under different classes and will not create confusion for customers. Each joint owner is entitled to use, license, charge or assign its right in the trademark without the consent of the other joint owners.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Trade secrets are protected against unauthorised disclosure, misuse and appropriation under competition laws in China. It is also provided in employment contract law that employees are responsible for keeping the trade secrets of their employer confidential. Trade secrets are defined as any technology information or business operation information that:

- is unknown to the public; can bring about economic benefits to the owner;
- has practical utility; and
- the owner has adopted security measures in.

Serious infringement of trade secrets can be deemed a criminal offence in China.

Trade secrets are kept confidential during court proceedings. Cases involving trade secrets can be heard in private if a party so requests.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brands can be protected as registered trademarks in China. Other branding factors, such as trade names, commercial appearance, product packaging and decoration, can be protected from plagiarism under competition laws in China.

Certain branding, such as logos and stylised marks, can also be protected by design rights and may also be protected by copyright as artistic works.

All registered trademarks are publicly announced upon registration and recorded in the trademark database of the China National Intellectual Property Administration and can be publicly searched. It is highly advisable for fintech businesses to conduct trademark searches to check whether earlier registrations exist that are identical or similar to their proposed brand names. It may also be advisable to conduct internet searches for any unregistered trademark rights that are also recognised and protected in China, which may prevent use of the proposed mark.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

Remedies include preliminary and final injunctions, damages or an account of profits, destruction of infringing products, and costs.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

There is a competition regime in China that applies to all entities carrying out business in China. However, there are no particular aspects of this regime that would affect fintech businesses disproportionately to other businesses.

The Guidelines for Anti-Monopoly in the Field of Platform Economy were issued by the Anti-monopoly Commission under the State Council on 7 February 2021. The Guidelines intend to set principles for preventing monopoly and investigating wrongdoings, taking into account the nature and characteristics of the platform economy. The State Administration of Market Regulation (SAMR) has initiated several high-profile cases against platform giants. Large fintech platforms are potential enforcement targets, too.

The Amendment to the Anti-Monopoly Law took effect on 1 August 2022 (Amendment). One key update is the express prohibition on monopolistic activities by using advantages in data, algorithm, technology, capital and platform rules. In March 2023, the SAMR issued the revised Provisions on Prohibiting the Abuse of Dominant Market Position, to further clarify the anti-monopoly rules for platform economy.

In recent years, high-level officials with the People's Bank of China and the former China Banking and Insurance Regulatory Commission have stated publicly that the 'winner-takes-all' situation of large fintech companies may lead to monopoly and discourage innovation, and that the competent regulators shall intensify supervision and enforcement.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

There are no tax incentives specifically applicable to fintech companies. However, there are some incentives and government support policies applicable to IT and high-tech companies, tech start-ups and their investors. These industrial policies and incentives are found across different regions of China.

In addition, there are also tax incentives available for some financial sector companies (which could be fintech companies), if they meet certain conditions. For example, the interest income of a microloan company's lending to farmers is entitled to value added tax exemption and income tax reduction until the end of 2023.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

There are no new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in China.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

There are no immigration schemes specifically for fintech talent, but the National Foreign Experts Bureau together with another two government authorities jointly issues a notice in January 2018, encouraging foreign scientists, specialised talents and highly skilled technical

talents to come and work in China. Eligible applicants can be issued visas that are valid for five to 10 years with multiple entries.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

Following the promulgation of the Data Security Law and the Personal Information Protection Law (PIPL) in late 2021, various Chinese regulators, including but not limited to the former China Banking and Insurance Regulatory Commission, have expressed that they would intensify enforcement actions against non-compliant data processing activities. The Fintech Development Plan (2022–2025) points out that, among others, China will make a series of supporting regulations and policies to implement the Cybersecurity Law, the Data Security Law and the PIPL in the fintech area.

There are also increasing discussions around fintech ethics, especially in relation to algorithm discrimination, intrusion of privacy and excessive collection of user data. Government policies issued in recent years have emphasised the ethical governance of fintech, and fintech ethics committees have been set up under local financial administrations in multiple cities and provinces. In October 2022, the People's Bank of China issued the Guidance on Scientific and Technological Ethics for the Financial Sector, setting out ethical rules about innovation, data security, inclusive service, transparency, fair competition, risk control and environmental, social and corporate governance.

More traditional players in the financial sector, including large banks, insurance companies and securities companies are actively advancing business digitalisation.

simmons+simmons

Jingyuan Shi jingyuan.shi@simmons-simmons.com
Yuchen Lai yuchen.lai@simmons-simmons.com
Yanyu Lai yanyu.lai@simmons-simmons.com

10/Floor China Construction Science and Industry Building,
3331 Zhongxin Road Nanshan, Shenzhen 518000, China
Tel: +86 755 8656 7720
www.simmons-simmons.com

Read more from this firm on Lexology

Read this article on Lexology

Denmark

Rasmus Mandøe Jensen and Jónas Már Torfason
Plesner Advokatpartnerselskab

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 129
General innovation climate 129
Government and regulatory support 130

FINANCIAL REGULATION 130
Regulatory bodies 130
Regulated activities 131
Consumer lending 133
Secondary market loan trading 134
Collective investment schemes 134
Alternative investment funds 135
Peer-to-peer and marketplace lending 136
Crowdfunding 136
Invoice trading 136
Payment services 136
Open banking 137
Robo-advice 137
Insurance products 137
Credit references 137

CROSS-BORDER REGULATION 138
Passporting 138
Requirement for a local presence 138

SALES AND MARKETING 138
Restrictions 138

CRYPTOASSETS AND TOKENS 139
Distributed ledger technology 139
Cryptoassets 140
Token issuance 140

ARTIFICIAL INTELLIGENCE 140
Artificial intelligence 140

CHANGE OF CONTROL 141
Notification and consent 141

Read this article on Lexology

FINANCIAL CRIME 141
Anti-bribery and anti-money laundering procedures 141
Guidance 141

DATA PROTECTION AND CYBERSECURITY 142
Data protection 142
Cybersecurity 142

OUTSOURCING AND CLOUD COMPUTING 143
Outsourcing 143
Cloud computing 143

INTELLECTUAL PROPERTY RIGHTS 143
IP protection for software 143
IP developed by employees and contractors 144
Joint ownership 145
Trade secrets 146
Branding 146
Remedies for infringement of IP 147

COMPETITION 147
Sector-specific issues 147

TAX 148
Incentives 148
Increased tax burden 148

IMMIGRATION 149
Sector-specific schemes 149

UPDATE AND TRENDS 150
Current developments 150

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

In recent years, the fintech sector has experienced significant growth in Denmark. This has been facilitated by:

- a highly educated and digitally literate population;
- a high degree of digitisation of public sector systems;
- the support of specific government policies aimed at promoting fintech innovation; and
- the development of Copenhagen as an international fintech hub.

Under the auspices of Copenhagen Fintech, a dedicated fintech lab opened in Copenhagen in 2016 and has become a central hub for fintech activity in Denmark.

In the past few years, a number of partnerships between fintech start-ups and banks have been announced, which reflects the current trend of fintech companies seeking to partner and cooperate with existing financial sector bodies rather than attempting to be in competition with and in opposition to them.

While there has been significant activity in traditional fintech core areas such as payments and investment services, ancillary areas such as regtech and insurtech remain less developed, but are expected to grow in the future.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

The government has specific policies aimed at promoting fintech business and investments and to support Copenhagen as an international fintech hub. Recently, this has resulted in increased funding for the Danish Financial Supervisory Authority (FSA), enabling it to dedicate resources to a specialised fintech office and create a regulatory sandbox. The FSA opened applications for its regulatory sandbox in 2018 and has published notes on projects examined in the regulatory sandbox as recently as September 2022, where a blockchain-based securities trading and clearing solution was examined.

In terms of purpose and eligibility criteria, the sandbox is similar to the existing one operated by the UK Financial Conduct Authority.

The FSA moreover operates a fintech forum where a wide range of industry interests are represented. The forum meets twice yearly.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

The main financial regulator is the Danish Financial Supervisory Authority (FSA), which also oversees compliance with anti-money laundering regulations.

Compliance with certain business conduct rules and other consumer and competition-oriented rules is overseen by the Competition and Consumer Authority.

The Data Protection Agency oversees compliance with data protection rules.

The Central Bank has limited oversight over systemically important payment and securities clearing and settlement infrastructures and similar systems.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Banking

Deposit-taking activities generally require a banking licence under the Financial Business Act to legally operate in Denmark. There are no de minimis or similar exemptions available.

Lending does not require a licence in Denmark, although a registration under the Act on Measures to Prevent Money Laundering and Financing of Terrorism may be required (as described below). However, under the FSA's current guidance, EU banking institutions may have to passport their licence into Denmark if they wish to perform lending activities there.

The Act on Consumer Loan Undertakings creates an exception to the licence-free lending requirement in Denmark, to the extent that the loan constitutes consumer credit.

Payment services or e-money issuance

The performance of payment services, as defined in the Annex to the Payments Act implementing Annex I to revised EU Directive 2015/2366/EU (Payment Services Directive) (PSD2), requires a licence under the Payments Act.

The Payments Act generally reflects the catalogue of exemptions to the licence requirement in article 3 of PSD2 and article 1 of EU Directive 2009/110/EU (Second EU Electronic Money Directive) (EMD2), except that technical services covered by the exemption in article 3(j) of PSD2 are subject to certain fee regulations in the Payments Act.

Specifically, regarding the limited network exemption (article 3(k) of PSD2 and article 1(4) of EMD2), although limited network products are exempted from the licence requirement, they must still comply with the disclosure, business conduct and fee rules of the Payments Act, as well as the regulation on issuance and redemption of e-money (corresponding mainly to Titles III and IV of PSD2 and article 11 of EMD2). However, the disclosure, business conduct and fee rules do not apply to e-money issued within a limited network if:

- the instrument cannot load a value of more than 3,000 Danish kroner;
- the instrument cannot be reloaded; and
- the issuer's aggregate outstanding e-money liabilities do not exceed an amount equivalent to €5 million, in which case only the rules on redemption of e-money apply.

Denmark has not elected to use the options in article 32 of PSD2 and article 9 of EMD2 to exempt low-volume and low-value payment services or e-money from the licensing requirement; however, the Payments Act provides for a less burdensome licensing process for such providers and issuers, which are also exempt from the own funds requirements.

Foreign exchange

Unless performed by a licensed bank, foreign exchange activities require a licence under the Act on Measures to Prevent Money Laundering and Financing of Terrorism. Exemptions

Read this article on Lexology

from certain parts of the Act are available for entities whose foreign exchange activities are de minimis – including a requirement that the foreign exchange business does not account for more than 5 per cent of the entity's aggregate annual turnover – and purely ancillary to their main business.

In addition, providers of exchange services between virtual and fiat currencies are subject to regulation under the Act just as such operators are required to be registered under the Act.

Investment activities

The provision of 'investment services' and the carrying out of 'investment activities' – both as defined in EU Directive 2014/65/EU (Markets in Financial Instruments Directive II) (MiFID II) – as well as the provision of custody services trigger a licensing requirement under Danish law, pursuant to the Danish Act on Investment Firms and Investment Services and Activities, which implements MiFID II and EU Directive 2019/2034/EU (Investment Firms Directive).

The Danish implementation of the Investment Firms Directive narrowly follows the wording of the Investment Firms Directive, but also includes certain specific national rules including in respect of, inter alia, certain restrictions on the provision of ancillary services, a rule on 'good business practices', the requirement to include 'Investment Firm' in the legal name of the investment company and the applicability of non-disclosure agreements.

Investment advice

Undertakings that provide investment advice must be licensed as an investment adviser if they do not hold another licence that permits them to provide investment advice. Investment advisers may also receive and transmit orders.

Financial advice

Undertakings that provide advice on financial products to consumers must be licensed as financial advisers. For this purpose, 'financial products' are credit agreements, excluding residential credit agreements, deposits, insurances, pension and investment products. 'Investment products' are transferable securities, units or shares in collective investment schemes, deposits in banks where the return depends on the performance of one or more underlying assets, guarantee certificates, cooperative certificates and mortgage deeds.

Residential credit intermediation

Undertakings that provide advice on or arrange or facilitate residential credit agreements to consumers must be licensed as residential credit intermediaries. Residential credit agreements essentially cover the granting of loans secured on real estate.

Alternative investment funds

The management of alternative investment funds triggers a registration or licensing requirement depending on the size of the assets of the managed investment fund. The threshold for authorisation rather than registration is assets under management by the manager of €100 million (or €500 million if certain conditions are complied with). Authorised managers must

comply with all of the requirements of the legislation implementing EU Directive 2011/61/EU (Alternative Investment Fund Managers Directive) (AIFMD), whereas a registered manager must comply with only a few limited requirements.

The definition of 'alternative investment funds' has been implemented from the AIFMD without material changes.

Insurances

Insurance activities generally trigger a licensing requirement. The Financial Business Act provides certain specific exemptions to the licensing requirement, none of which would be expected to be relevant for fintech businesses.

If the activity does not amount to being an insurer but involves insurance distribution, the activity will require a licence if it constitutes insurance or reinsurance mediation. There are no exemptions to this requirement. On the other hand, intermediaries that perform only ancillary insurance intermediation must be registered.

In general, the Danish market has seen only a limited number of insurtech providers, including Undo, which has entered into a partnership with Danish insurance provider Tryg and Penni and has previously worked with the Danish insurance provider TopDanmark.

Anti-money laundering

Fintech businesses that are not otherwise required to have a licence under any of the above regulations must be registered with the FSA if they perform any of the activities set out in Annex I to the Act on Measures to Prevent Money Laundering and the Financing of Terrorism, including:

- deposit-taking;
- lending;
- financial leasing;
- assistance in offering securities and services ancillary thereto; and
- the storage, administration and management of securities.

Additionally, providers of various cryptocurrency-related services, including the providers of crypto exchanges and cryptocurrency wallets, as well as issuers of cryptocurrencies, must be registered under the Act on Measures to Prevent Money Laundering and the Financing of Terrorism.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

The Act on Consumer Loan Undertakings creates an exception to the absence of a requirement for a licence to lend in Denmark. The Act applies to most types of consumer loan and credit agreements unless:

- they are provided by an already licensed bank or other financial business;

- the agreement is for a zero-interest and zero-fee loan; or
- the agreement is a leasing agreement without any obligation to purchase.

Under the Act on Consumer Loan Undertakings, consumer loan and credit in-scope providers must obtain a licence from the FSA (during which, the management of the consumer loan undertaking will be subject to customary fit and proper requirements) and will be subject to ongoing conduct of business rules.

The Act includes a 35 per cent cap on the annual percentage rate (APR) on consumer loans, including on peer-to-peer loans; a cap on expenses (eg, interest, fees and reminder charges) over the life of the credit of 100 per cent of the original principal amount; and a prohibition on marketing consumer loans with an APR of more than 25 per cent as well as any marketing of consumer loans in connection with gambling or betting, or both (subject to limited exceptions, including marketing on the credit provider's own website).

However, in respect of online marketing directed at consumers, the above-mentioned marketing prohibition will not apply to consumer loan undertakings located in other EU countries. To the extent that the marketing by these foreign consumer loan undertakings is carried out on television or on-demand services or in connection with gambling or betting, or both, the marketing prohibition will apply.

The Danish parliament recently passed a bill in which buy now, pay later (BNPL) credit will be regulated as consumer loans, with few exceptions. These exceptions include:

- deferral of payment by a vendor (without a third-party credit provider) for up to 90 days after delivery of the product or service; and
- payment cards with a credit line, where payment is settled within 50 days of the transaction.

The legislation enters into force on 1 July 2023.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

There are no restrictions on trading loans in the secondary market under Danish law.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Fintech companies providing such financial products or services are not subject to any bespoke regulation. However, to the extent that their services constitute a regulated activity pursuant to the generally applicable regulatory regime, these companies fall within the scope of the relevant regulation.

Read this article on Lexology

Depending on the nature of the activity, fintech businesses may be subject to one or more of the following laws, each of which includes associated delegated regulations:

- the Payments Act (implementing PSD2 or EMD2), if the activity involves offering payment services or issuing e-money;
- the Investment Association Act (implementing EU Directive 2009/65/EU (Undertakings for Collective Investment in Transferable Securities), if the activity involves establishing or managing undertakings for collective investment in transferable securities;
- the Act on Alternative Investment Fund Managers (implementing the AIFMD), if the activity involves establishing or managing an alternative investment fund;
- the Capital Markets Act and EU Regulation No. 2014/596 (Market Abuse), to the extent that a crowdfunding scheme constitutes equity crowdfunding, thereby subjecting the fintech business to the rules regulating, among other things, offerings of securities and prospectus requirements; or
- Regulation (EU) 2020/1503) (European Crowdfunding Service Providers) if the activity involves the matching of business funding interests of investors and project owners through the use of a crowdfunding platform that consists of either:

    - the facilitation of granting of loans; or
    - placing without a firm commitment basis of transferable securities and admitted instruments for crowdfunding purposes issued by project owners or a special purpose vehicle as well as the reception and transmission of client orders in relation to those transferable securities and admitted instruments for crowdfunding purposes.

In respect of crowdfunding lending platforms, lenders engaging on the platform are – regardless of whether the lenders are professional lenders or acting in a private capacity – subject to a cap of 35 per cent of the annual percentage rate on such loans, if the borrower is a consumer.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

As Denmark is an EU member state, the AIFMD applies.

The management of alternative investment funds triggers a registration or licensing requirement depending on the size of the assets of the managed investment fund. The threshold for authorisation rather than registration is assets under management by a manager of €100 million (or €500 million if certain conditions are complied with). Authorised managers must comply with all of the requirements of the legislation implementing the AIFMD, whereas a registered manager must comply with only a few limited requirements.

The definition of 'alternative investment funds' has been implemented from the AIFMD without material changes.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Such types of alternative financing are not subject to bespoke regulation in Denmark. However, whether they are professional lenders or acting in a private capacity, the lenders using the platform and the loans provided by them over the platform are subject to a cap of 35 per cent of the annual percentage rate on these loans if the borrower is a consumer.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

If the crowdfunding scheme in question constitutes 'donation-based crowdfunding', the rules set out in the Danish Fundraising Act may apply. Additionally, depending on the structure of the crowdfunding scheme, the Danish Capital Markets Act and the EU Market Abuse Regulation may apply, to the extent that a crowdfunding scheme constitutes equity crowdfunding, thereby subjecting the fintech business to the rules regulating, among other things, offerings of securities and prospectus requirements.

The European Crowdfunding Service Providers Regulation applies if the activity involves the matching of business funding interests of investors and project owners through the use of a crowdfunding platform that consists of either:

- the facilitation of granting of loans; or
- placing without a firm commitment basis of transferable securities and admitted instruments for crowdfunding purposes issued by project owners or a special purpose vehicle as well as the reception and transmission of client orders in relation to those transferable securities and admitted instruments for crowdfunding purposes.

Non-bank lending or equity crowdfunding vehicles have a relatively limited market share.

Invoice trading

11 Describe any specific regulation of invoice trading in your jurisdiction.

Invoice trading is not subject to bespoke regulation. However, to the extent that the relevant invoice-trading scheme constitutes a factoring arrangement, such factoring arrangements are subject to the Anti-money Laundering Act and would trigger a registration requirement with the FSA, as well as a requirement to comply with the other provisions set out in the Act.

Payment services

12 Are payment services regulated in your jurisdiction?

The performance of payment services, as defined in the Annex to the Payments Act implementing Annex I to PSD2, requires a licence under the Payments Act.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

No, except the rules implementing articles 65 to 68 of PSD2. The Payments Act contains rules that severely restrict the processing and use of payment data.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Robo-advice is not subject to specific regulation in Denmark. In July 2019, the FSA published a regulatory note regarding best practice when using supervised machine learning.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Insurance activities generally trigger a licensing requirement. The Financial Business Act provides certain specific exemptions to the licensing requirement, none of which are considered relevant for fintech businesses.

If the activity is not of a scale for the provider to be considered an insurer but involves insurance distribution, the activity will require a licence if it constitutes insurance or reinsurance mediation. There are no exemptions to this requirement. On the other hand, intermediaries that perform only ancillary insurance intermediation must be registered.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Credit information services and credit information bureaus must generally adhere to the rules set out in the EU General Data Protection Regulation and the Danish Data Protection Act. Credit information bureaus must seek a licence from the Danish Data Protection Agency prior to the commencement of any data processing.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

Yes, to the extent that the entity is an EU or EEA entity and the underlying EU law provides for a passporting system.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

In general, obtaining a Danish licence (as opposed to passporting an existing licence) for financial services requires that the applicant be domiciled in Denmark.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

The laws and regulations that govern and restrict the sale and marketing of financial services and products in Denmark include:

- the Act on Alternative Investment Fund Managers (implementing EU Directive 2011/61/EU (Alternative Investment Fund Managers Directive);
- EU Directive 2014/65/EU (Markets in Financial Instruments Directive);
- the Consumer Contracts Act (implementing parts of EU Directive 2011/83/EU on Consumer Rights and EU Directive 2002/65/EU (Distance Marketing of Consumer Financial Services), which contains rules on pre-contractual information requirements, right of withdrawal, termination and binding periods; and
- the Marketing Practices Act (implementing EU Directive 2005/29/EU (Unfair Commercial Practices), which – in addition to the rules implementing the EU Unfair Commercial Practices Directive – contains rules on, among other things:
    - unsolicited marketing;
    - comparative advertisements;
    - the marketing of consumer credit;
    - Consumer Ombudsman activities; and
    - how businesses must comply with good marketing practices.

The Marketing Practices Act also (subject to limited exceptions, including marketing on the credit provider's own website) prohibits marketing of consumer loans with an annual percentage rate of more than 25 per cent and all marketing of consumer loans in connection with gambling or betting, or both.

Read this article on Lexology

- The Payments Act (implementing EU Directive 2015/2366/EU (Payment Services), which contains rules implementing the disclosure, business conduct and fee rules set out in Titles III and IV of the Directive and corresponding provisions of EU Directive 2009/110/EU (Second EU Electronic Money Directive).
- The Credit Contracts Act (implementing parts of EU Directive 2008/48/EU (Consumer Credit Directive)), which applies to credit arrangements with consumers and that contains, among other things:

    - mandatory disclosure requirements;
    - rules on changes to interest rates;
    - walk-away rights; and
    - rules on term and termination.

- The Act on Consumer Loan Undertakings, which applies to certain forms of loan and credit to consumers provided by lenders that are not banks or other forms of licensed financial business.
- The Executive Order on Good Business Practices for consumer loan and credit providers issued pursuant to the Act on Consumer Loan Undertakings, which contains rules on duty of care to customers, a prohibition against aggressive or misleading market practices, marketing restrictions and restrictions on amending or terminating consumer loan and credit contracts.
- The Executive Order on Good Business Practices for Financial Businesses (implementing parts of EU Directive 2011/83/EU (Consumer Rights Directive), which contains rules on duty of care to customers, disclosure requirements, advising customers and restrictions on amending or terminating customer contracts and applies to, among others:

    - banks;
    - mortgage banks; and
    - investment firms.

- The Executive Order on Good Business Conduct for Insurance Distributors (implementing parts of EU Directive 2016/97/EU (Insurance Distribution Directive)), if the activity involves insurance distribution.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

Distributed ledger technology and blockchain are not subject to bespoke regulation in Denmark. The European Union, however, has passed a regulation comprised of a six-year pilot regime on distributed ledger market infrastructure, which sets out the requirement on multilateral trading facilities and securities settlement systems using distributed ledger technology (DLT) and amends the existing definition of 'financial instruments' pursuant to EU Directive 2014/65/EU (Markets in Financial Instruments Directive II) to include such instruments issued by means of DLT.

Read this article on Lexology

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

Crypto assets and digital currencies are not subject to bespoke Danish regulation. Digital wallets and e-money are subject to the EU rules pursuant to revised EU Directive 2015/2366/EU (Payment Services Directive).

Providers of the following crypto-asset services are required to be registered with the Danish FSA pursuant to the Act on Measures to Prevent Money Laundering and the Financing of Terrorism:

- providers of exchange between cryptocurrencies and fiat currencies;
- custodian wallet providers;
- providers of exchange between different cryptocurrencies;
- providers of transfer services of cryptocurrencies;
- issuers of cryptocurrencies.

In addition, the EU regulation of markets in crypto-assets (MiCA), which includes regulation specifically aimed at utility-tokens, stablecoins and e-money tokens, is expected to enter into force during the course of 2025 (with rules on stablecoins expected to enter into force in the second half of 2024).

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Issuers of cryptocurrencies fall under the Act on Measures to Prevent Money Laundering and the Financing of Terrorism and are required to be registered with the Danish FSA. The MiCA, which includes regulation specifically aimed at 'crypto-asset service providers', which includes digital currency exchanges and brokerages.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

Artificial intelligence (AI) is not subject to bespoke regulation in Denmark. In July 2019, the Danish Financial Supervisory Authority (FSA) published a regulatory note regarding best practice when using supervised machine learning. Further, on 21 April 2021, the European Commission published a proposal for a directive to regulate artificial intelligence that aims

Read this article on Lexology

to promote the development of artificial intelligence and address the risks it poses to safety and fundamental rights.

On 17 May 2023, the FSA published for discussion a draft best-practices document for data ethics while using AI within the financial sector.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

In general, if a regulated business changes control, this triggers a notification or a consent requirement from the Danish Financial Supervisory Authority (FSA). This includes businesses and undertakings subject to the regulations set out in the Financial Business Act. Further, to the extent that a company must register with the FSA pursuant to the Anti-money Laundering Act, there would be a de facto consent requirement from the FSA in the event of a change of control, as the FSA can revoke a registration if it considers that the company or the management of the company no longer meets the requirements under the Anti-money Laundering Act.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Fintech businesses that require a licence under the Financial Business Act, the Payments Act, the Alternative Fund Managers Act or the Act on Financial Advisers, Investment Advisers and Residential Credit Intermediaries or require a licence to carry out insurance activities, investment services or the provision of investment or financial advice are subject to the rules set out in the Act on Measures to Prevent Money Laundering and the Financing of Terrorism. This also applies to fintech businesses carrying out activities as a foreign exchange and cryptocurrency-related services (and not otherwise subject to regulatory requirements under the Financial Business Act).

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

No guidelines have been made available at this time that specifically target fintech companies. However, the Danish Financial Supervisory Authority (FSA) has prepared and published guidelines to the Act on Measures to Prevent Money Laundering and the Financing of Terrorism, which can be found on the Danish FSA website.

Read this article on Lexology

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

EU Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR) and the Danish Data Protection Act (DDPA) apply to fintech products and services if personal data is processed. The regulations apply to all data processing relating to an identified or identifiable natural person (eg, name, account and credit card information, other customer identification data and internet protocol address). The DDPA supplements the GDPR with national Danish rules, including special rules on the processing of national identification numbers (ie, the Danish Central Person Registration number).

Fintech products and services that involve the processing of personal data on behalf of another company (ie, the customer or data controller) require that a written data processing agreement is entered into. Further, if data is transferred outside the European Union, a legal basis for the transfer must be in place.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

Financial businesses (eg, banks, investment firms and insurers), payment institutions and e-money institutions must generally have prudent IT and cybersecurity systems, procedures and policies. However, apart from these general regulatory requirements, there are no generally applicable statutory cybersecurity regulations or standards.

Further, particularly within payment services, there are a number of important IT and cybersecurity standards, including:

- the Regulatory Technical Standards on Strong Customer Authentication and Common and Commission Delegated Regulation (EU) 2018/389 (Secure Open Standards of Communication);
- the Guidelines on the Security Measures for Operational and Security Risks of Payment Services (promulgated under revised EU Directive 2015/2366/EU (Second Payment Services Directive); and
- the payment card industry (PCI) IT industry security standards, particularly the PCI Data Security Standard and the PCI Payment Application Data Security Standard.

Although these are widely accepted industry standards, they do not constitute public law regulations and as such are not directly enforced by the Financial Supervisory Authority.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

The Executive Order on Outsourcing of Material Areas of Activity (the Outsourcing Order) sets out the legal requirements relating to the outsourcing by a financial services company of a material aspect of its business. In addition to the Outsourcing Order, the Danish Financial Supervisory Authority (FSA) has published regulatory guidance on its requirements.

The purpose of the Outsourcing Order is, inter alia, to align the Danish outsourcing rules with the outsourcing guidelines of the European Banking Authority. The Outsourcing Order contains some national gold-plating provisions (eg, regarding outsourcing to cloud service providers), which go beyond the outsourcing guidelines of the European Banking Authority.

The Outsourcing Order sets out specific requirements for the outsourcing of 'critical or important' areas, including detailed requirements for the outsourcing agreement between the company and the outsourcing provider (eg, requirements for the description of the outsourced activity and whether the outsourcing provider may sub-outsource the activity to a third party). The Outsourcing Order also covers the outsourcing of capital and liquidity risk management, outsourcing of IT and security and outsourcing of key functions.

The Danish FSA has published official guidelines to the Outsourcing Order.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

In addition to the Outsourcing Order and the related FSA regulatory guidance on the Outsourcing Order, Danish financial services companies use the European Banking Authority guidelines on outsourcing as guidance.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Fintech innovations may be protected as inventions under patent law if they are patentable. This includes filing for a patent and meeting the requirements under Danish patent laws (eg, patentable subject matter, novelty and inventive step). Fintech innovations may also be protected as utility models where the bar for protection is lower than that of a patent.

Further, if the innovation is embodied in software coding, copyright protection may be available to the author (in this case, the programmer) if the software coding has a sufficient degree of originality. In addition, fintech innovations may be protected as sui generis database rights if the conditions for protection set out in section 71 of the Copyright Act (incorporating EU Directive 96/9/EU (Legal Protection of Databases)) are met.

Although not intellectual property in the traditional sense, a fintech innovation may be protected as a trade secret under the Trade Secrets Act (incorporating EU Directive 2016/943/EU (Protection of Undisclosed Know-How and Business Information (Trade Secrets) (Trade Secrets Directive) if the innovation is kept secret.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Copyright

The Danish Copyright Act stipulates that the person who creates a work owns the copyright to that work. This applies regardless of whether the person is an employee or a contractor or consultant.

In relation to copyright created during the term of employment, the general rule is that there is an automatic transfer of copyright from the employee to the employer by virtue of the employment provided certain criteria are met. The employer shall only be entitled to the parts of the employee's copyright that were necessary for the employer's usual activities at the time when the employee created the work. Further, it is a condition that the employment is of a permanent nature and that creating the work was part of the employee's tasks.

Moreover, the copyright to computer programs developed by an employee, within the scope of his or her employment or as a result of the employer's directions, automatically transfers in full to the employer.

Inventions (patents and utility models)

If a person (eg, an employee or a consultant) has made a technical invention that can be patented or registered as a utility model, the starting point is that the employee or the consultant is entitled to this invention.

Pursuant to the Danish Employees' Inventions Act, if the invention has been made as part of the employment, the employer is entitled to claim that the right to the invention be transferred to them if the use of the invention falls within the scope of the activities of the company.

The same applies if the employee's invention relates to a specific task assigned to him or her by the employer. Even if the invention was made during off-duty hours, the employer could still be entitled to claim the right to the invention. The Danish Employees' Inventions Act does not apply to consultants.

Read this article on Lexology

The Act on Inventions at Public Research Institutions regulates the right to inventions made by teachers and other scientific employees at universities. The Act stipulates that the employee is entitled to an invention that he or she has made him or herself; however, the Act also states that the institution has a right to claim that this invention be transferred to it, if the employee made the invention as part of his or her work.

Designs

The right to a design depends on whether it is a Danish design or a community design. The Danish Designs Act stipulates that the person who created the Danish design or the person to whom the designer's right has been transferred has the right to acquire the exclusive right to the design.

The Danish Designs Act does not regulate the relationship between employer and employee. It is, however, assumed that under the Danish Designs Act, the design rights belong to the employer, unless the design is also protected by copyright. In the latter case, the design right follows the copyright and is determined based on an analogy of the rules on copyright for employees (see above).

According to article 14(3) of the Regulation on Community Designs, any rights to a community design shall vest in the employer unless otherwise agreed or specified under national law. This only applies to traditional employment relationships (employer–employee). For commissioned designs, the question of whom the rights belong to must be decided specifically.

Trademarks

The trader, and not the person who created the sign, owns the rights to the sign. If an employee owns the copyright or design rights to the sign, the employer can only use it if they have agreed on this or if it is otherwise justified under the copyright and design rules. Accordingly, it is important to determine whether the employee created the trademark as a part of his or her work or whether the exploitation of the trademark falls within the scope of the usual activities of the employer.

If a consultant owns the copyright to the sign, the trader will have a right of use only unless otherwise agreed.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

As the joint ownership of IP rights is commonly regulated on a contractual basis between the joint owners, restrictions on a joint owner follow from the contractual regulation thereof.

If an invention is made jointly, each person will own a proportionate share of the invention in the absence of a prior agreement. The joint ownership entails some restrictions on each person's right to use, license, charge or assign the invention, even without an agreement.

In general, all joint owners of an invention must agree on substantial decisions regarding the jointly owned invention, including agreements on licensing. Each owner may individually sell or assign its own share in the invention unless otherwise agreed.

With regard to copyright, co-authors to a copyrighted work, where each contribution cannot be separated as independent works, enjoy joint co-ownership in the copyright of the work.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Confidential information and trade secrets are covered by the Trade Secrets Act (incorporating the Trade Secrets Directive and the Danish Penal Code.

With regard to the confidentiality of trade secrets (including confidential information) during court proceedings, the Trade Secrets Act stipulates that the duty of confidentiality to which the court's staff (eg, the judge), lawyers and others employed by the law firm are subject, implies that the unlawful use or disclosure of trade secrets that the person in question has learned about through involvement in or access to the legal proceedings is a punishable offence. This also applies to other persons involved in the legal proceedings, such as witnesses.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

The most relevant IP rights protecting branding are set out in the Trademarks Act, the Marketing Practices Act and the Copyright Act.

The Trademarks Act protects signs used in branding, such as brand names, mottos or catchphrases and logos. The Marketing Practices Act protects certain commercial signs that have the necessary degree of distinctiveness. Copyright protection may in principle be afforded under the Copyright Act for user interfaces in software and website designs, which may enjoy copyright protection with regard to branding; however, in practice, this protection is difficult to obtain.

Trademark protection in Denmark may be obtained by way of both a community (EU) trademark and on the national level in Denmark as a Danish trademark. In Denmark, trademark protection may be obtained by way of both registration and use-based rights. To be registered as a trademark, the trademark owner must be able to reproduce the trademark in an appropriate manner by using technology that is generally available to determine the content of the trademark right clearly and precisely. Protection under the Marketing Practices Act is obtained by use, when the necessary degree of distinctiveness exists.

To avoid trademark infringement of existing brands, fintech businesses should perform appropriate freedom-to-operate analysis prior to launching brands, including checking both

national and EU registers for potentially conflicting registered rights. As protection in some cases can be established by use, a market check is also necessary. Similarly, as regards the Marketing Practices Act, where protection is also established formlessly, a market check is necessary.

The Danish Patent and Trademark Office can, in connection with a trademark application, produce a search report showing rights with which the applicant may come into conflict. However, the owners of these prior rights are not automatically notified of this and, thus, it is up to each owner to stay informed and assess whether they believe their rights are infringed.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

A number of remedies are available to individuals or companies whose IP rights have been infringed, including:

- financial compensation (eg, damages and reasonable remuneration);
- injunctions (eg, preliminary injunctions);
- corrective measures;
- the publication of judicial decisions;
- reasonable compensation for legal costs; and
- criminal penalties.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

The fintech nature of a product or service does not in itself give rise to particular competition law issues.

However, aspects of the fintech business model mean that certain competition law considerations – of general application – often become relevant in the context of fintech businesses.

One example of this is the widespread use of partnerships between fintech businesses and incumbent financial institutions that, depending on the nature of the partnership, may raise competition law questions about horizontal or vertical cooperation.

At the other end of the spectrum, where a fintech product or service requires the fintech business to access a financial institution's systems or customer data and the financial institution is reluctant to provide this access, questions of anti-competitive behaviour may arise in certain circumstances.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

Danish tax law provides no specific fintech incentives, but there are specific incentive rules concerning R&D:

- a temporary – but expected to be permanent – regime provides for a 130 per cent tax deduction of R&D costs, maximised within a group to 910 million Danish kroner annually; and
- a tax credit regime – whereby it is possible for smaller start-ups to convert a tax loss, to the extent it is created by R&D costs, into cash from the Danish state. It only applies to R&D costs of up to 25 million Danish kroner annually, namely, a maximum annual payout of 5.5 million Danish kroner.

Danish tax law also contains general tax incentives in the form of tax-favourable treatment on granting shares, options and warrants, where a company can grant up to 10 per cent (or 20 per cent – and even 50 per cent for small businesses – if certain requirements are met) of an employee's remuneration through such instruments. These favourable tax incentives have in part been introduced to promote start-up businesses in Denmark.

Danish tax law also includes an expat tax regime under which foreign employees may be taxed by 32.84 per cent of their remuneration for up to seven years. The tax regime only applies if certain requirements are met. These are – among others – salary requirements (in excess of 72,500 Danish kroner (in 2023) per month after deduction of the Labour Market Supplementary Pension), not having been involved in the management of the employer company and not having been taxable in Denmark. The use of the expat tax regime requires registration with the Danish tax authorities. The expat tax regime is part of retaining and attracting highly qualified foreign employees.

On a broader scale, the Danish government published their political objectives on 14 December 2022. These included an allocation of 300 million Danish kroner to support the Danish entrepreneurial sector through a strategy with an emphasis on, for example, ease of access to foreign workforce, retaining the 130 per cent tax deduction of R&D costs and regulations explained above and other initiatives to aid the Danish start-up ecosystem.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

There are no such proposed tax laws currently implemented or underway.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

Citizens from other EU and EEA countries or Switzerland may work in Denmark under the EU rules on the free movement of persons and services. As a clear starting point, citizens from outside of the European Union, the European Economic Area and Switzerland must have a work permit to work in Denmark. Subject to certain conditions, such citizens may also work in Denmark under the EU rules on the free movement of services.

There are several immigration schemes aimed at the recruitment of skilled staff. However, none are specific to the technology or financial sector. The most relevant schemes for a fintech business are:

- the Pay Limit Scheme, which ensures that an employee is granted a work permit if their annual salary is over a certain amount (465,000 Danish kroner in 2023) and the employment terms correspond to Danish standards;
- the Supplementary Pay Limit Scheme, under which an employee is granted a work permit if the following conditions are met:

    - their annual salary is over a certain amount (375,000 Danish kroner in 2023;
    - the employment terms correspond to Danish standards;
    - the offered job position has been posted on Jobnet and the EURES portal;
    - the seasonally adjusted gross unemployment in Denmark does not exceed 3.75 per cent; and
    - the employee has not received a fine of 3,000 Danish kroner or more under the Criminal Code or the Aliens Act; and

- the Positive List scheme, under which residence and work permits are granted to employees who have been offered jobs that are listed on one of the Positive Lists covering certain professions and fields that are currently experiencing a shortage of qualified professionals. The list contains more than 100 professions and is available on the Danish Immigration Service website; and
- the Fast-Track Scheme, which makes it faster and easier for certified companies to recruit foreign employees with special qualifications to work in Denmark.

Additional immigration schemes are available that may be relevant (eg, for trainees or intra-group secondments).

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

No.

PLESNER

Rasmus Mandøe Jensen rmj@plesner.com
Jónas Már Torfason jomt@plesner.com

Amerika Plads 37, Copenhagen 2100, Denmark
Tel: +45 33 12 1133
www.plesner.com

Read more from this firm on Lexology

Read this article on Lexology

Egypt

Mohamed Hashish and Farida Rezk
Soliman, Hashish & Partners

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 152
General innovation climate 152
Government and regulatory support 153

FINANCIAL REGULATION 154
Regulatory bodies 154
Regulated activities 154
Consumer lending 155
Secondary market loan trading 155
Collective investment schemes 156
Alternative investment funds 156
Peer-to-peer and marketplace lending 156
Crowdfunding 157
Invoice trading 157
Payment services 157
Open banking 158
Robo-advice 158
Insurance products 158
Credit references 159

CROSS-BORDER REGULATION 159
Passporting 159
Requirement for a local presence 159

SALES AND MARKETING 159
Restrictions 159

CRYPTOASSETS AND TOKENS 160
Distributed ledger technology 160
Cryptoassets 160
Token issuance 160

ARTIFICIAL INTELLIGENCE 160
Artificial intelligence 160

CHANGE OF CONTROL 161
Notification and consent 161

Read this article on Lexology

FINANCIAL CRIME 161
Anti-bribery and anti-money laundering procedures 161
Guidance 161

DATA PROTECTION AND CYBERSECURITY 162
Data protection 162
Cybersecurity 162

OUTSOURCING AND CLOUD COMPUTING 162
Outsourcing 162
Cloud computing 163

INTELLECTUAL PROPERTY RIGHTS 163
IP protection for software 163
IP developed by employees and contractors 164
Joint ownership 164
Trade secrets 164
Branding 164
Remedies for infringement of IP 165

COMPETITION 165
Sector-specific issues 165

TAX 166
Incentives 166
Increased tax burden 166

IMMIGRATION 167
Sector-specific schemes 167

UPDATE AND TRENDS 167
Current developments 167

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Fintech is governed by several Egyptian laws and regulations, including the following main laws and regulations (as amended):

- the Non-cash Payment Methods Law No. 18 of 2019;
- the E-signature Law No. 15 of 2004 and its Executive Regulation;
- the Non-Financial Markets and Instruments Law No. 10 of 2009;
- the Microfinance Law No. 141 of 2014;
- the Trade Code No. 17 of 1999;
- the Consumer Finance Law No. 18 of 2020;
- the Cybercrime Law No. 175 of 2018;
- the Investment Law No. 72 of 2017 and its Executive Regulation;
- the Consumer Protection Law No. 181 of 2018 and its Executive Regulation;

Read this article on Lexology

- the Small and Microenterprises Law No. 141 of 2004 and its Executive Regulation;
- the Telecoms Law No. 10 of 2003;
- the Media Law No. 180 of 2018;
- the Capital Market Law No. 95 of 1992 and its Executive Regulation;
- the Movable Securities Law No. 115 of 2015 and its Executive Regulation;
- the Anti-Money Laundering Law No. 80 of 2002 and its Executive Regulation;
- the Public Entities Contracts Law No. 182 of 2018 and its Executive Regulation;
- Presidential Decree No. 89 of 2017, founding the National Payments Council;
- the Banking Law No. 194 of 2020 (the Banking Law);
- the Data Protection Law No. 151 of 2020 (the Data Protection Law); and
- the Non-Banking Financial Services Law No. 5 of 2022 (the Fintech Law).

Fintech was not regulated in Egypt until the issuance of the Banking Law. The Banking Law addresses the regulation of several fintech sectors, which includes digital banks, crypto-currency and e-payments. The current government of Egypt has promoted and continues to promote financial inclusion and the digitalisation of the financial sector in Egypt. In February 2022, the new Fintech Law came into force under Law No. 5 of 2022. The aim of the Fintech Law is to facilitate the integration of technologies into financial services and formulate a regulatory framework for fintech businesses to support non-banking financial services. It covers services such as robo-advisory, microfinance, insurtech, artificial intelligence, mobile applications and digital platforms. The Executive Regulation of the Fintech Law came into force in April 2022, applying the procedures and conditions for a Fintech Licence under the Fintech Law.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

In May 2019, the Central Bank of Egypt (CBE) launched a regulatory sandbox for the purpose of providing fintech players with a virtual space within which, subject to a specific framework, applicants can experiment with their solutions for a limited period of time on a small scale and under a well-defined parameter.

Furthermore, a number of funding initiatives are available to fintech start-ups in Egypt. For example, in March 2019, the CBE launched the Fintech Innovation Fund with a value of 1 billion Egyptian pounds. In April 2019, the International Finance Corporation launched, in collaboration with two local partners in Egypt, a two-year programme to support the fintech space in Egypt, and the World Bank Group set aside US$200 million for small and medium-sized enterprises in Egypt, which can also be used by small and medium-sized fintech players.

In response to the covid-19 pandemic, the CBE organised the distribution of free point-of-sale terminals, eased fees and charges and increased contactless payment limits. In November 2020, the e-invoicing system was launched.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

Several bodies are responsible for enforcing fintech-related laws and regulations, including:

- the CBE, which is empowered by Law No. 88 of 2003 on the Central Bank of Egypt and the Banking Sector (Banking Law No. 194 of 2020) to, among other things, regulate bank accounts and banking transactions;
- the Information Technology Industry Development Agency, which is empowered by the E-signature Law No. 15 of 2004 to, among other things, promote and develop the information technology and communications industry, support small and medium-sized enterprises in using e-transactions and regulate e-signature services activities;
- the Financial Regulatory Authority (FRA), which is empowered by the Non-Financial Markets and Instruments Law No. 10 of 2009 to, among other things, license the carrying out of non-banking financial activities and the protection of stakeholders within the non-banking financial market; it is also empowered by the new Fintech Law to issue licences to non-banking financial services who use fintech;
- the National Payments Council, which is empowered by Presidential Decree No. 89 of 2017 to, among other things, reduce the use of cash outside the banking sector, support and encourage the use of electronic methods and channels instead of cash, and protect the consumers of any payment systems and services; and
- the National Telecommunications Regulatory Authority, which is generally empowered by Telecoms Law No. 10 of 2003 to regulate and enhance telecommunication services.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

In general, according to the Banking Law and several judgments issued by the economic courts, neither natural nor juristic persons may practise any banking activity in Egypt without being licensed by and registered with the CBE except for public legal persons who carry out any such work within the limits of their establishment.

'Banking activities' are defined under the Banking Law, as 'banking business: every activity that mainly and habitually deals with accepting deposits, obtaining financing and investing these funds in providing financing and credit facilities or contributing to the capital of companies' funds and all that takes place in banking custom as a bank business'. This definition is also adopted by the Trade Code No. 17 of 1999.

Any person that violates these provisions is subject to imprisonment or a fine of not less than 1 million Egyptian pounds and not more than 10 million Egyptian pounds, in accordance with the Banking Law. There are two main prerequisites that must be satisfied to apply such penalties with respect to any banking activity, namely carrying out the banking activity on a regular basis and having the banking activity as the main activities of any person, including individuals and juristic persons.

Read this article on Lexology

Other than the aforementioned general rule, each of the following activities is also regulated and subject to licensing requirements in Egypt:

- microfinancing;
- investment banking;
- brokerage;
- factoring;
- foreign exchange trading;
- payment services;
- e-commerce;
- financial leasing;
- mortgage finance; and
- consumer lending.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

The Consumer Finance Law No. 18 of 2020 was issued on 16 March 2020, governing any activity aimed at financing the purchase of products or services for consumption purposes as long as the activity will be carried out on a regular basis. Among the activities covered is financing through payment cards or any other means decided by the CBE.

The aforementioned consumer finance-related activities may not be carried out in Egypt unless a licence is obtained from the FRA. The licence requires, among other things, the carrying out of the activities by a joint-stock company with an issued capital of at least 10 million Egyptian pounds.

The Consumer Finance Law (including the licensing requirement) does not apply to all banks registered with the CBE nor any entity licensed to carry out mortgage financing, financial leasing, factoring, microfinancing or the purchasing of properties from real estate developers.

The Consumer Finance Law applies only to vehicles, durable products, educational services, medical services, travel, and leisure services as well as any other products and services that are determined by the FRA.

Secondary market loan trading

6 | Are there restrictions on trading loans in the secondary market in your jurisdiction?

In general, there are no restrictions on trading loans in Egypt. However, if the trading is being carried out on a regular basis, then it may be deemed as carrying out banking activities, in which case licensing by and registration with the CBE is required.

The assignment of debts in Egypt is subject to a specific legal framework to be effective in respect of debtor and surety (if any).

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

As a general rule, no activity relating to investment funds may be carried out unless a licence is obtained from the FRA. Banks registered with the CBE may carry out such activity, provided that the relevant approval is obtained from the CBE.

Investment funds may, in general, be established in the form of a joint-stock company with a minimum issued capital of 5 million Egyptian pounds or its equivalent in any currency.

Licensed investment funds must deposit any securities that they are investing in one of the banks that are registered with the CBE, provided that the bank (and its related parties) does not control or hold more than 10 per cent of the total shares of the investment fund company.

One of the licensing requirements to be qualified for the investment fund underwriting is to have the minimum required infrastructure and technology to do so.

Investment funds may take the form of an open-end fund, closed-end fund, private equity fund, exchange-traded fund, money market fund, debt fund, real estate fund, donor-advised fund or related fund.

Promoting investment funds is generally not allowed prior to establishing them except for in the case of private equity funds and provided that, among other things, a notification is sent to the FRA and that no underwriting is made as part of the promotion.

Most of the alternative financial products and services that are provided by fintech companies generally fall within the scope of either collective investment schemes or banking activities.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Managers of alternative investment funds are regulated, including board members.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Peer-to-peer and marketplace lending can be deemed as banking activities, in which case licensing by and registration with the CBE is required in accordance with the Banking Law.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

Crowdfunding falls within the definition of banking activities; however, it may also be a form of a donor-advised fund.

In practice, a number of donor-advised funds have been established by a special presidential decree rather than a licence from the FRA. For example, Presidential Decree No. 139 of 2014 established a fund of a private nature called the Tahya Misr Fund for the purpose of assisting the government in, among other things, establishing development and service projects as well as developing slums and micro and small projects.

The government has used the crowdfunding approach to fund a number of public utility projects, such as the crowdfunding that was used in 2014 to fund the development of the New Suez Canal, which cost Egypt approximately 30 billion Egyptian pounds.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

Invoice trading may be characterised under Egyptian law as a banking activity (if providing credit), and may also be characterised as factoring. However, this can be assessed on a case-by-case basis.

Licensed factors are allowed to provide, among other things, guarantee, collection and account management services.

The following three main conditions are required in the subject of any factoring transaction:

1 it must be created from a commercial transaction related to the relevant buyer and debtor but not through cash financing;
2 it must not be associated with any third party's existing or future right; and
3 it must not be limited or restricted unless otherwise agreed by the relevant factor and buyer.

The subject may also be fully depreciated, provided that points (2) and (3) are satisfied.

The provisions of the Banking Law and several judgments issued by the economic courts also apply to factoring.

Payment services

12 | Are payment services regulated in your jurisdiction?

There is a specific regulation governing payment services that are provided by technical payment aggregators or payment facilitators. Services agreements are subject to specific know-your-customer and anti-money laundering checks and must include specific terms

and conditions for those services, including a restriction on subcontracting unless certain conditions are met.

Under the Banking Law, no activity concerning the operation of a payment system or the provision of a payment system may be carried out unless a licence is obtained by the CBE. This new restriction applies to all persons, whether natural or juristic, carrying out the activity in Egypt or providing the services from abroad to any residents in Egypt, with the exception of stock exchanges, futures exchanges, securities settlement systems, licensed central clearing, depository and registry systems, custodian banks and internal systems of the Egyptian Ministry of Finance that do not include payment, collection, setting-off or clearance of payment.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

The CBE recently introduced a set of regulations regarding open banking, which govern instant payment network services in Egypt. This new regulation allows people to make electronic payments between bank accounts using their mobile phones via application programming interfaces (APIs). However, a licence must be obtained from the CBE by banks wishing to provide such services.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

The new Fintech Law and its Executive Regulation introduced regulations on robo-advisers, which are subject to licensing by the FRA.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

According to the Insurance Law No. 10 of 1981, no one is allowed in person or through an intermediary to carry out any activity related to insurance or reinsurance in Egypt without obtaining a licence from the FRA. Fintech companies that sell or market insurance products fall within the scope of this restriction and are regulated in Egypt.

Furthermore, the new Fintech Law and its Executive Regulation also regulates insurtech, which is subject to licensing by the FRA.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

All services relating to the provision of credit rating and indebtedness references are regulated. Such services require a licence from the CBE.

At present, there is only one licensed company, namely the Egyptian Credit Bureau, that is subject to a specific legal framework governing the provisions of those references.

In general, disclosing credit ratings and indebtedness references related to any person is not allowed unless approval is obtained from the relevant person.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

Not applicable.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

Fintech companies cannot obtain a licence to provide financial services in Egypt without first establishing a local presence.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

In general, the sales and marketing of financial services and products in Egypt are regulated and subject to prior licensing and approval.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

There are no specific regulations or rules applied to distributed ledger technology or blockchains. However, Banking Law No. 194 of 2020 (the Banking Law) prohibits the issuance or trade of cryptocurrencies or electronic money and the creation or operation of platforms for their trading without obtaining a licence from the Central Bank of Egypt (CBE) in accordance with the rules and procedures it specifies.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

The Banking Law prohibits the issuance or trade of cryptocurrencies or electronic money and the creation or operation of platforms for their trading without obtaining a licence from the CBE in accordance with the rules and procedures it specifies.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

There is no specific regulation governing STOs or ICOs in Egypt.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

There is no special regulation in Egypt governing artificial intelligence. However, in accordance with Prime Ministerial Decree No. 2889 of 2019, a new national council was established called the Artificial Intelligence National Council (AINC). The AINC is empowered to determine, supervise, and follow up on Egypt's national strategy for artificial intelligence in light of international developments.

In addition, since 2019, the Minister of Higher Education has begun adding special artificial intelligence departments to several engineering universities in Egypt.

Read this article on Lexology

The government has created an enabling legal environment to govern the uses of artificial intelligence. This involves the issuance of the Data Protection Law, in July 2020, which regulates the relationship between data owners and users.

Furthermore, robo-advice is now newly regulated under the Fintech Law and is subject to licensing from the Financial Regulatory Authority.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Notification and consent requirements depend on several elements, such as the type and location of business that is the subject of the change of control. For example, no one is allowed to acquire between 5 and 10 per cent of the issued capital of any bank registered with the Central Bank of Egypt (CBE) unless a notification is sent to the CBE. Prior approval from the CBE is required to acquire more than 10 per cent of the issued capital. A similar restriction applies to insurance companies.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Money laundering is mainly governed by the Anti-Money Laundering Law No. 80 of 2002 (the AML Law) and its Executive Regulation.

The AML Law names 15 entities that must comply with its provisions and its Executive Regulation, including all banks, branches of foreign banks in Egypt and money transfer entities.

Those entities are also subject to several obligations under other laws governing their specific activities. Violating these obligations will result in imposing different penalties including fines or imprisonment, or both.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

All available guides can be found on the anti-money laundering page of the Central Bank of Egypt's website.

Read this article on Lexology

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The Data Protection Law No. 151 of 2020 (the Data Protection Law) applies to any personal data that is subject to electronic processing, whether partially or entirely.

The Data Protection Law generally prohibits the transfer of personal data to a foreign country without first obtaining a licence from the new regulatory authority for personal data protection – typically referred to as the Data Protection Centre – and where the level of protection is less than what is provided for by the Data Protection Law. The policies and regulations for cross-border transfer shall be specified by the Executive Regulations, which have not yet been issued. After the date of its issuance, any entity subject to the Data Protection Law is required to legitimise its position within one year.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

According to Cybercrime Law No. 175 of 2018, all providers of information technology and telecommunications services, including the processing or storing of data, must retain and store users' data for at least 180 continuous days, including identification, the content of the services' system, communication traffic, terminals and any other data required by the National Telecommunications Regulatory Authority.

The providers must also keep all stored and archived data (including personal data) confidential and not disclose the data unless there is a court order to do so.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

There are specific legal requirements and regulatory guidance for the outsourcing of specific services. For example, online trading is subject to specific regulations requiring brokerage companies to satisfy certain conditions and requirements to provide any trading solutions online, which include specific technical requirements and conditions on the information technology infrastructure of the brokerage companies.

Another example, according to a circular issued by the Central Bank of Egypt (CBE) in 2014, is that no bank registered with the CBE may provide internet banking solutions, including online lending, unless prior authorisation is obtained from the CBE. This prior authorisation

Read this article on Lexology

requires all banks registered with the CBE to meet specific legal requirements, including the provision of a penetration test report to the CBE.

According to Banking Law No. 194 of 2020 (the Banking Law), the board of directors determines the important services that are provided to banks such as outsourcing and technical services, and it has the right to set the conditions and procedures for registering their providers with the CBE, provided that they include, in particular, determining the minimum that must be met with regard to governance requirements, risk management, service performance standards and controls for maintaining confidentiality.

Banks are prohibited from seeking assistance from providers of such services who are not registered with the CBE, and the bank shall be fully responsible for these actions.

According to the Banking Law, delegated services are defined as the services delegated by licensed entities to third parties to perform certain functions and services on their behalf. Accordingly, these delegated service providers must register with the CBE.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

Cloud computing is subject to the Cybercrime Law No. 175 of 2018, which applies to any person providing users, directly or indirectly, with any information technology and telecommunications service, including processing or data storage. Such providers must retain and store users' data for at least 180 consecutive days, including identification, the content of services' system, communication traffic, terminals and any other data required by the National Telecommunications Regulatory Authority.

According to the Media Law No. 180 of 2018, a prior licence from the Supreme Council for Media Regulation is required to launch any website in Egypt if:

- the website will be created in Egypt;
- the website will be managed by any person in Egypt; or
- any of the website's subdomains will be managed by any person in Egypt.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Software is protected in Egypt in the form of copyright. This protection requires the registration of the software, including, among other things, the first and final 10 pages of the source code, with the Information Technology Industry Development Agency.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

According to Intellectual Property Rights Law No. 82 of 2002 (the IPR Law), only the person who provides the direction to create a joint work is entitled to exercise the author rights of the work. This rule applies to copyright created by employees during the course of their employment.

For contractors and consultants, it depends on the specific terms and conditions of the relevant development or services agreement.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

According to the IPR Law, if there is more than one author of any work, all participants in the work are considered joint authors, and none of them can individually exercise any right over the work unless otherwise agreed by the authors in writing.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Trade secrets (including confidential information) are protected by the IPR Law, provided that the secrets:

- are maintained as confidential and are not within the public domain;
- maintain their value as a result of their confidential status; and
- maintain their confidentiality status under the effective protection measures taken by their owner.

According to the IPR Law, the court will maintain the confidentiality of trade secrets.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Branding is generally protected as both copyright and trademark.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

There are several remedies under Egyptian law for owners of intellectual property rights, including specific performance and the right to claim damages to cover all the losses incurred by the owner as well as all the profits of which the owner has been deprived as a result of the infringement.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

To assess whether there is an antitrust-related risk, it must first be determined whether the relevant fintech player is deemed to be in a dominant position in accordance with the meaning given under the Antitrust Law No. 3 of 2005 as amended and its Executive Regulations (the Antitrust Law).

For a fintech player and its controlled affiliates in Egypt to be deemed to be in a dominant position under the Antitrust Law, the player must:

1 hold a market share exceeding 25 per cent of the market that is relevant to each service provided by the player (the relevant market), the percentage being calculated based on two elements, namely the relevant products (the relevant market products) and the geographic area during a certain period;
2 be able to make an impact on changing the prices or the quantity of the market products (the dominant ability); and
3 not be in a position to limit the dominant ability, noting that the competitors have the ability to carry out the same business as the fintech player in Egypt whether at present or in the future.

Points (2) and (3) are reviewed and assessed by the Egyptian Competition Authority (ECA) based on specific criteria.

If the fintech player is in a dominant position in the relevant market, then that player must be in a position to conduct certain practices, including entering into any agreement with any of its suppliers or customers that results in limiting competition.

The assessment of any violation under the Antitrust Law is made by the ECA on a case-by-case basis according to specific criteria, including, among other things, the benefits of customers and commercial customs. The assessment is subject to a judicial review by the economic courts.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

The Investment Law No. 72 of 2017 provides fintech companies, subject to the satisfaction of specific criteria, with several key guarantees and incentives, including:

- exemption from stamp duty and the notarisation fee imposed on articles of incorporation, facilities and loans agreements, security documents or plot of land purchase agreements for five years, starting from the date of registration with the Commercial Registry;
- application of a unified custom duty at a flat rate of 2 per cent of the value of any equipment, machinery and device that is necessary for establishment of the investment projects; and
- tax reduction for seven years, from the date of starting the investment projects in Egypt, subject to a specific formula.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

The Egyptian Tax Authority (ETA) is currently in the process of proposing several amendments to the existing tax regimes in Egypt, whereby a new digital tax will be introduced. However, it is too early to know the rates of the proposed digital tax.

On 26 March 2020, the Minister of Finance issued Decree No. 188 of 2020 introducing a mandatory clearance e-invoicing framework where all issued invoices must be digitally transmitted to the ETA in real time before being sent to the customer. The decree obliges all value added tax-registered businesses to issue an electronic invoice containing the issuer's electronic signature and a unified code for the goods or services.

On 2 August 2020, the ETA issued Decree No. 386 of 2020 listing 134 companies who are obliged to issue electronic tax invoices for their sold goods or rendered services as of 15 November 2020. This date is the first phase of a broader roll-out of the e-invoicing obligation. In addition, voluntary adoption of the e-invoicing system is permitted if certain conditions and controls are satisfied.

On 20 November 2020, the ETA issued Decree No. 518 of 2020 listing 347 companies, as a second phase, who are obliged to issue electronic tax invoices for their sold goods or rendered services as of 15 February 2021. It was announced through the media that, by the end of June 2021, the e-invoicing system would be mandatory for all companies.

Furthermore, Decree No. 125 of 2021 with regard to the e-invoicing implementation requires all companies registered with the ETA regardless of their size, to issue their invoices electronically from 15 February 2022.

Read this article on Lexology

According to the Ministry of Finance, value added tax is no longer deductible from paper invoices as of January 2022.

It is also worth noting that, according to Decree No. 188 of 2023, when determining the net commercial and industrial taxable profits of financiers registered in the electronic tax invoice system, only electronic invoices shall be considered in proving deductible costs and expenses as of 1 July 2023, with the exception of paper invoices previously issued by financiers and written before the date of their obligation to issue electronic tax invoices.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

As a general rule, non-Egyptians are not allowed to work in Egypt without being permitted to do so by the Ministry of Manpower. In practice, the issuance of a work permit takes up to three months and is valid from one to three years.

The proportion of foreign employees must not exceed 10 per cent of the total number of employees and must not exceed 20 per cent of the company's payroll. The 10 per cent threshold may be increased to 20 per cent for fintech businesses subject to specific criteria.

UPDATE AND TRENDS

Current developments

41 Are there any other current developments or emerging trends to note?

The issuance of the new Fintech Law is the first set of regulations in Egypt governing the integration of technology into financial services such as robo-advisory, microfinance, insurtech, artificial intelligence, mobile applications and digital platforms.

Furthermore, in May 2022, the Central Bank of Egypt (CBE) announced its intention to start rolling out digital banking licences in accordance with Banking Law No. 194 of 2020 (the Banking Law). Since the issuance of the Banking Law in 2020, five banks have applied and have been waiting for their digital banking licence. These banks are the National Bank of Egypt, Banque Misr, Emirates NBD, Qatar National Bank and the Arab Banking Corporation.

The CBE revealed that it is studying the application of Central Bank Digital Currency (CBDC). As stipulated by the CBE, such CBDC is safe and stable as an alternative to other types of cryptocurrencies and to mitigate the risks arising with regards to digital financial services. This constitutes part of the measures taken by CBE against the spread and circulation of cryptocurrencies.

Read this article on Lexology

The CBE also announced that it is currently working on developing the regulatory framework for licensing digital banks.

SOLIMAN, HASHISH & PARTNERS
LAW FIRM

Mohamed Hashish m.hashish@shandpartners.com
Farida Rezk f.rezk@shandpartners.com

2nd Floor, Plot No.15, Ninetieth Street, New Cairo, Egypt
Tel: +202 2812 4499
www.shandpartners.com

Read more from this firm on Lexology

Read this article on Lexology

Germany

Christopher Götz, Daniel Kendziur, Jochen Kindermann, Sascha Kuhn and Sascha Morgenroth*

Simmons & Simmons

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 170

General innovation climate 170
Government and regulatory support 171

FINANCIAL REGULATION 171

Regulatory bodies 171
Regulated activities 171
Consumer lending 172
Secondary market loan trading 173
Collective investment schemes 173
Alternative investment funds 173
Peer-to-peer and marketplace lending 174
Crowdfunding 175
Invoice trading 175
Payment services 175
Open banking 176
Robo-advice 176
Insurance products 176
Credit references 177

CROSS-BORDER REGULATION 177

Passporting 177
Requirement for a local presence 177

SALES AND MARKETING 177

Restrictions 177

CRYPTOASSETS AND TOKENS 178

Distributed ledger technology 178
Cryptoassets 178
Token issuance 179

ARTIFICIAL INTELLIGENCE 179

Artificial intelligence 179

CHANGE OF CONTROL 181

Notification and consent 181

Read this article on Lexology

FINANCIAL CRIME	**181**
Anti-bribery and anti-money laundering procedures	181
Guidance	183
DATA PROTECTION AND CYBERSECURITY	**183**
Data protection	183
Cybersecurity	185
OUTSOURCING AND CLOUD COMPUTING	**186**
Outsourcing	186
Cloud computing	186
INTELLECTUAL PROPERTY RIGHTS	**187**
IP protection for software	187
IP developed by employees and contractors	187
Joint ownership	188
Trade secrets	188
Branding	190
Remedies for infringement of IP	190
COMPETITION	**190**
Sector-specific issues	190
TAX	**193**
Incentives	193
Increased tax burden	194
IMMIGRATION	**195**
Sector-specific schemes	195
UPDATE AND TRENDS	**196**
Current developments	196

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

The fintech landscape has developed further during the past year. The high speed of regulatory changes requires firms to adjust to this developing landscape. They have to evaluate whether to deal with the demanding regulatory hurdles and with this get access to the whole German market including institutional investors or to stay outside of Germany.

Several market participants have already achieved the goal of becoming authorised in Germany and there are still a substantial number of applications pending with the German Federal Financial Regulatory Authority (BaFin). The high number of applications underlines the strength and relevance of the German market.

It is also interesting to note that in particular in the cryptosphere many of the traditional players now jump on this trend as well. The gap between traditional and new players in this

Read this article on Lexology

respect became smaller, which is in line with the approach that BaFin always took (namely, that new fintech players should not be treated differently from existing market participants if they offer the same product).

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

The German government and municipalities support fintech companies in various ways. BaFin is the financial regulatory authority in Germany. BaFin set up a dedicated team to support fintech companies in relation to their market entry, and it also organises events (eg, the annual BaFin-Tech conference) to discuss regulatory developments with market participants. Although fintech companies do not benefit from special treatment, BaFin supports fintech companies in relation to evaluating licensing requirements and clarifying ongoing regulatory aspects. The German Ministry of Finance has appointed experts to a special FinTech counsel, the FinTechRat, which offers support and counsel to the legislator when further working on a suitable regulatory framework. On a municipality level, all German cities that consider themselves hubs for fintech (eg, Berlin, Frankfurt, Munich and Hamburg) offer additional support through fintech centres. In addition, universities in or around fintech centres tend to support and dedicate resources to the development of an effective fintech ecosystem, as do institutions like the Leibniz Institute for Financial Research. However, there are no regulatory sandboxes available in Germany.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

The German Federal Financial Regulatory Authority (BaFin) is responsible for regulating fintech products and services in Germany if they fall under the scope of regulated activities or products.

Regulated activities

4 Which activities trigger a licensing requirement in your jurisdiction?

According to German law, anyone wishing to conduct banking business or to provide financial services or investment services in Germany commercially or on a scale that requires a commercially organised business undertaking requires a written licence from BaFin. What constitutes banking business, financial services or investments services is set out in the Banking Act and the Securities Institutions Act and includes, among other things:

- deposit business;
- debenture business;
- lending business;
- discount business;

Read this article on Lexology

- principal broking business);
- security deposit business;
- activities of a central securities depositor;
- the obligation to repurchase previously sold loan receivables prior to their maturity;
- guarantee business;
- cheque collection business;
- underwriting business;
- business of a central counterparty;
- investment brokerage;
- investment advice;
- operation of a multilateral trading facility;
- placement business;
- operation of an organised trading facility;
- contract broking;
- financial portfolio management;
- trading on own account;
- non-EEA deposit brokerage;
- crypto custody business;
- foreign currency dealing;
- factoring;
- financial leasing;
- investment management;
- limited custody business; and
- proprietary trading.

Since the beginning of 2020, the crypto-custody business has been added to the list of licensable activities. Crypto-custody business is defined as the safekeeping, administration and storage of cryptoassets or private cryptographic keys used to hold, store and transfer cryptoassets for others (cryptoassets custody services).

In general, a licence is required for any investment services and activities listed in section A of Annex I of Directive 2014/65/EU (Markets in Financial Instruments Directive II) or Annex I of Directive 2013/36/EU (Capital Requirements Directive). The provision of payment services is licensable based on the provisions of the German Act on the Supervision of Payment Services, which implements Directive 2007/64/EC (Payment Services Directive) and

Directive (EU) 2015/2366 (revised Payment Services Directive) (PSD2) into German law.

The trading of claims deriving from fully drawn loan agreements does not trigger a licence requirement, provided that the claim is not amended. However, amendments requiring a new credit decision (eg, prolongation) can constitute a licensable lending business.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

The contractual basis for consumer lending contracts can be found in the German Civil Code. The civil law provisions contain an elaborate protection regime and require the borrower to comply with, among other things, certain disclosure obligations and walk-away rights for

the borrowers. In particular, the licence requirement is triggered if the repayment obligation is in cash. Where the repayment obligation takes the form of financial instruments or other goods or rights, other licensing requirements may apply (eg, investment services).

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

In general, the trading of fully drawn loans does not trigger a licensing requirement in Germany. Restrictions on the trading of loans may apply under the terms of the respective contract or as a result of data protection rules.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

The German Capital Investment Code (KAGB) provides the licensing and supervision regime for investment management companies and investment funds in Germany. In addition, the marketing of investment funds to investors in Germany is also regulated under the KAGB. The KAGB takes a holistic approach and provides the legal regime for all collective investment schemes (eg, alternative investment funds and undertakings for collective investments in transferable securities). The aim of the KAGB is to ensure an adequate supervision of collective investments, including the administration, marketing and compliance with investment rules. However, crowdfunding platforms and peer-to-peer (P2P) lending platforms are generally not viewed as collective investment schemes by BaFin. BaFin focuses on the lending aspect and indicates in several guidance notes that, depending on the actual nature of the services provided, licensable lending business may be conducted. Further, the brokerage of loans requires a licence under the German Industrial Code and, therefore, the operation of a P2P lending platform could trigger the requirement for a loan broker licence. Further, Regulation (EU) 2020/1503 (Crowdfunding Regulation) is directly applicable law in Germany.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Managers of alternative investment funds (AIFs) located in Germany are regulated under the KAGB. The same also applies to a certain extent to German branches of non-German managers of AIFs. AIFs may only be marketed in Germany once they are registered or passported for distribution to investors in Germany. Germany has implemented Directive 2011/61/EU (Alternative Investment Fund Managers Directive).

Depending on the nature of their actual activities, fintech companies are generally outside the scope of the KAGB if their activities do not constitute the structuring and managing of an investment fund. An investment fund is, pursuant to section 1(1), sentence 1 of the KAGB, any collective investment scheme that raises capital from a number of investors, with a view

to investing in accordance with a defined investment policy for the benefit of those investors and that does not constitute an undertaking operating outside of the financial sector. Such a number of investors will be deemed to exist if the fund rules or the articles of association of the collective investment fund do not limit the number of potential investors to a single investor.

However, since 3 June 2023, the new German Regulation on Crypto Fund Units allows the distribution of fund units or shares on a tokenised basis. This is a significant step and opens new distribution channels for fund managers as well as fintech companies.

Further, the KAGB has been amended and allows German special AIFs (broadly a fund whose investors must be legal persons) to invest up to 20 per cent of the total assets of the special AIF to be invested in cryptoassets. This also provides new investment opportunities for investment managers who are interested in investing in cryptoassets.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Lenders and borrowers

BaFin has published guidance on the question of when the participants of a P2P marketplace typically conduct lending or deposit business on a scale that triggers a licensing requirement. According to this guidance, BaFin assesses potential licence requirements on a case-by-case basis, taking into account the activities of every single investor. It is particularly important that investors do not invest on a commercial scale or in a manner that would require a commercially organised business undertaking, because otherwise a banking licence requirement is triggered. BaFin suggests that a commercially organised business undertaking is required if more than €500,000 is invested or more than 100 loans are granted. An investor invests on a commercial scale if he or she undertakes the investments for a certain time and with a view to making a profit. In addition, under certain circumstances, crowd-lending models are subject to the Act on Capital Investments, so that several investor protection rules apply, such as the requirement to produce a sales prospectus, which must be approved by BaFin. However, exemptions may apply.

P2P or platform operators

Whether the operation of a crowd-lending platform requires a licence (and which kind of licence) depends on the actual services that are provided. Generally, it depends on the way the contracting is designed on the platform. In cases where the operator of the platform merely provides the infrastructure, the licensable activities are more likely to be conducted by the users of the platform. If, on the other hand, the operator of the platform steps into each transaction and takes on its own credit risk, it is likely that the licensable activity will be conducted by the platform operator. However, the pure brokerage of loans would generally not be considered as banking, financial or payment services, so 'only' an authorisation under the German Industrial Code may be required. It should, however, be kept in mind that the EU Crowdfunding Regulation is directly applicable law in Germany, hence, operators of crowdfunding platforms may require a licence. BaFin has created a task force

for crowdfunding providers that can be contacted if there are uncertainties with regard to possible licence requirements.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

There are several different kinds of crowdfunding platforms available in Germany. In a guidance note, BaFin sets out four main crowdfunding models:

- donation-based crowdfunding;
- rewards-based crowdfunding;
- loan-based crowdfunding (crowd lending or lending-based crowdfunding); and
- crowd investing (equity-based crowdfunding).

In the latter two types, the aim is to generate a financial return. BaFin does not apply specific regulatory regimes to different business models per se. BaFin instead focuses on the nature of the activities undertaken by the users and the operators of the crowdfunding platforms and decides on a case-by-case basis whether licensable activities are being conducted and by whom. It should, however, be kept in mind that the EU Crowdfunding Regulation is directly applicable law in Germany, hence, operators of crowdfunding platforms may require a licence. BaFin has created a task force for crowdfunding providers that can be contacted if there are uncertainties with regard to possible licence requirements.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

Invoice trading is generally not a regulated activity. However, if the actual activities constitute a financial service (eg, factoring, which means the ongoing purchase of receivables on the basis of standard agreements, with or without recourse) this activity is regulated and requires a financial services licence.

Payment services

12 | Are payment services regulated in your jurisdiction?

Germany has implemented PSD2 and, thus, anyone wishing to conduct payment services as a payment institution commercially or on a scale that requires commercially organised business operations needs written authorisation from BaFin. What constitutes payment services is set out in the German Act on the Supervision of Payment Services and comprises the same activities set out in PSD2.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

No, we are not aware of any such laws or regulations.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Robo-advice is any form of customer support on investment decisions by making use of partially or fully automated IT systems. There are several different kinds of automated investment advice platforms that are active in Germany. BaFin has issued guidance on robo-advice, indicating that these services can be qualified as (and regulated as) investment advice, financial portfolio management, acquisition brokerage and investment brokerage (each depending on its individual features), and, thus, offering respective services regularly requires licensing under German regulatory and commercial law. Most offerings currently available on the German market constitute investment advice or financial portfolio management.

In terms of their supervision and regulation, robo-advising businesses are generally subject to the same rules as if such services were rendered manually. Thus, automated investment advice will need to comply with the applicable licensing requirements and conduct of business rules. BaFin's guidance sets out that the provision of robo-advice could fall under a number of regulated services, including investment advice and contract brokering. Additionally, providers often offer portfolio management services under the label of robo-advice. Depending on the actual structure of the business, additional conduct of business rules may apply. For example, where the provider uses an advisory model and gives personalised recommendations to its investors, certain documentation obligations apply. In addition, the provider may need to determine the suitability and appropriateness of the financial products that it recommends.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Fintech companies selling or marketing insurance products in Germany are likely to be regulated by BaFin if they conduct insurance business in Germany and by the local chamber of industry and commerce if they act as insurance brokers in Germany.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Should a credit information service qualify as a credit-rating agency, the rules of Regulation (EC) No. 1060/2009 (Credit Rating Agency) apply.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

As Germany is a member of the European Union, institutions holding a licence to conduct regulated activities in any EEA country can apply for a passport. The passport is a notification procedure to the home state regulator. Such a passport would enable the licence holder to establish a physical presence in the form of a branch in the host country or to provide services on a cross-border basis without a physical presence. The passport avoids a complete authorisation procedure if a party intends to carry out a regulated activity in another EU country. Not all services can be passported. Cryptoassets custody services and asset management services are, for example, services that are not harmonised and will trigger a licence requirement when carried out in Germany.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

A German financial services licence will only be granted to a fintech company that has established a physical presence in Germany. However, a fintech company with a financial services licence in another EEA country can apply for a passport to Germany and, thus, would be able to provide financial services in Germany through a branch or without a physical presence on a purely cross-border basis.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

There are various restrictions regarding the sales and marketing of financial services and products in Germany. The marketing of a regulated activity in Germany constitutes a licensable activity and providing those services without the necessary licence constitutes a criminal offence. The marketing of financial instruments is subject to a detailed regulatory framework set out in Directive 2014/65/EU (Markets in Financial Instruments Directive II).

Read this article on Lexology

Providing false or misleading information is generally prohibited. Further rules apply for specific types of financial instruments like investment funds or publicly offered securities.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

No, there is no single regulation specifically addressing distributed ledger technology (DLT). However, the approach to regulatory requirements is technology agnostic. The use cases deploying DLT or blockchain technology in regulated markets (eg, securities markets) must comply with the existing legal framework applicable to the specific service and its providers. European requirements such as Regulation (EU) No 648/2012 (European Market Infrastructure Regulation) (EMIR), Regulation (EU) No. 600/2014 (Markets in Financial Instruments Regulation) (MiFIR), Regulation (EU) No. 909/2014 (Central Securities Depositaries Regulation), Directive 2014/65/EU (Markets in Financial Instruments Directive II) (MiFID 2), Directive 2011/61/EU (Alternative Investment Fund Managers Directive) and Regulation (EU) 2015/2365 (Securities Financing Transactions Regulation) as well as the national implementation thereto must be regarded provided the relevant product qualifies as a financial instrument. For instance, a case of use involving the clearing of assets by deploying DLT would have to fulfil the requirements of EMIR and MiFIR regarding authorisation and regulated entities. The German Federal Financial Regulatory Authority (BaFin) has the power to prohibit unauthorised businesses. In addition, smart contracts and initial coin offerings are currently under close scrutiny by the supervisory authorities. Other rules apply with regard to products that do not qualify as financial instruments within the MiFID 2 definition (eg, cryptocurrencies), here the Regulation on Markets in Cryptoassets (MiCA) provides the legal framework.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

Germany has implemented national regulations regarding cryptoassets that are not specifically focused on digital currencies. In particular, Germany has implemented crypto-custody business as a new financial service and added cryptoassets to the list of financial instruments.

Crypto-custody business is defined as the custody, management and protection of cryptoassets or private cryptographic keys used to keep, store or transfer cryptoassets for others.

- Custody in this context means taking care of cryptoassets as a service for third parties. This includes, in particular, service providers that hold cryptoassets of their customers collectively, without their customers being familiar with the cryptographic keys used. The intention here is primarily to protect clients against the risk the provision of wallets

may create (eg, loss of keys, fraudulent behaviour, etc). Management broadly means ongoing fulfilment of the rights resulting from the cryptoassets.

- Protection means both the digital storage of third parties' private cryptographic keys, which are provided as a service, and the safekeeping of physical data media (eg, a USB stick or a piece of paper) on which such keys are stored. The mere provision of storage space, for example, by web hosting or cloud storage providers, do not fulfil the definition unless these providers expressly offer their services for the storage of private cryptographic keys.

The distribution of cryptoassets requires authorisation by BaFin if the distribution is performed on a commercial basis or requires a commercially organised business operation. If virtual currencies are bought and sold for third parties, this could be classified as 'proprietary trading' under the German Banking Act, depending on the specific arrangements deployed, which requires a BaFin authorisation as well. In addition, e-money institutions must be authorised and subject to supervision by BaFin. Offering digital wallets online may require BaFin authorisation depending on the tokens and the wallet services being provided. BaFin has the power to prohibit any unauthorised business activities with immediate effect. MiCA will provide the legal framework for such activities as directly applicable law in Germany.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Yes. As set out above, Germany has implemented national regulations regarding cryptoassets that are not specifically focused on digital currencies.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

In Germany, there is no specific AI Act. Once the EU AI Act comes into force (draft proposal published in 2021), it will be directly applicable in Germany and will potentially have an impact on robo-advice services. Until then, robo-advice is governed by specific applicable rules in other legislation. There is also some guidance from authorities. In particular, the Federal Financial Supervisory Authority (BaFin) has actively addressed these regulatory aspects in the past; however, currently, this is an ongoing process. Starting in 2018, BaFin conducted a comprehensive study on the challenges and implications for supervision and regulation of AI-based and big data-based services, concluding that the proliferation of these technologies will increasingly challenge current regulatory frameworks. Besides ascertaining the need to adapt the supervisory framework accordingly, regulated companies remain accountable for regulatory compliance in AI-based and big data-based products. While management boards remain fully accountable for any results automatically produced

or used within their company (section 25a of the German Banking Act), these results must also remain transparent and explainable to ensure persisting human control. Thus, BaFin considers the use of black-box algorithms an indicator of dysfunctional (unlawful) business organisation. In addition, the accuracy and reliability of AI-based and big data-based products must be ensured. This, again, requires robust data quality, thorough testing and continuous supervision of algorithmic decision models, as well as technical safeguards against maldevelopment (eg, automated shutdown procedures).

Since late 2019, there has been increasing demand by various stakeholders in the German financial market for BaFin to engage in authorising the use of algorithms for automated decision-making. To date, this request remains unheard. BaFin announced that, apart from existing authorisation of individual scenarios (eg, article 142 et seq and article 362 et seq of Regulation (EU) No. 575/2013 (Capital Requirements Regulation), high-frequency trading), there is no legal basis for requiring or granting such authorisation on a general basis. BaFin has reaffirmed this in its 2021 publication 'Big data and artificial intelligence – use of algorithms for automated decision-making'.

Robo-advice is any form of customer support on investment decisions by making use of partially or fully automated IT systems. There are several different kinds of automated investment advice platforms that are active in Germany. BaFin has issued guidance on robo-advice, indicating that these services can be qualified as (and regulated as) investment advice, financial portfolio management, acquisition brokerage and investment brokerage (each depending on its individual features), and, thus, offering respective services regularly requires licensing under German banking (eg, the Banking Act and the German Securities Trading Act) and commercial law (eg, the German Industrial Code). Most offerings currently available on the German market constitute investment advice or financial portfolio management.

In terms of their supervision and regulation, robo-advising businesses are generally subject to the same rules as if such service was rendered manually. Thus, automated investment advice will need to comply with the applicable licensing requirements and conduct of business rules. BaFin's guidance sets out that the provision of robo-advice could fall under a number of regulated services, including investment advice and contract brokering. Additionally, providers often offer portfolio management services under the label of robo-advice. Depending on the actual structure of the business, additional conduct of business rules may apply. For example, where the provider uses an advisory model and gives personalised recommendations to its investors, certain documentation obligations apply. In addition, the provider may need to determine the suitability and appropriateness of the financial products that it recommends.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Investors that intend to acquire 10 per cent or more of the capital or the voting rights of a regulated entity are required to file a disclosure as holders of a significant holding. These investors must provide detailed information regarding their background, the origin of their funding, the CVs of relevant persons and the details of their group structure. The Federal Financial Supervisory Authority then generally has 60 days to approve or oppose the acquisition and may make approval subject to certain actions being taken.

In addition, notification requirements under securities trading or stock corporation laws may apply, depending on the legal nature of the target.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

First, a distinction must be made between anti-bribery and corruption (ABC) regulations and anti-money laundering (AML) rules.

As taking and giving bribes are criminal offences under the German Criminal Code, only individuals can be held criminally liable. Corporations and legal entities as such can solely be subject to regulatory investigations and sanctions. However, if the individual acts on behalf of a corporate body, the corporation may be subject to additional fines and confiscation of assets gained because of criminal conduct or forfeiture of other assets. All relevant administrative offences committed in Germany are mainly covered under the provisions of the Act on Regulatory Offences.

Thus, German regulatory offences law allows legal entities to be fined for bribery offences that have been committed by their legal representatives or by any other senior management employee, the conduct of whom can be associated with the legal entity. Fines of up to €600 million have been imposed for bribery offences in the past.

In contrast to this, all companies in Germany must generally comply with national AML regulations. In addition, where an institution is an obliged entity under section 2 of the German Money Laundering Act, it is under numerous additional obligations (eg, to set up a specific AML compliance system). This means that it is not – as with the ABC regulations – a matter of breach of criminal provisions by natural persons (eg, employees), but that the entity itself may violate the rules under the Money Laundering Act. For this reason, the corresponding sanctions also result directly from the law itself.

Read this article on Lexology

There have been some changes to the Money Laundering Act in the past including obligations especially for fintech companies. Institutions in the field of cryptoassets (eg, virtual currency exchange platforms and custodian wallet providers) are explicitly included in the group of obliged entities.

Generally, entities subject to German AML laws are, or will be required to, among other things:

- implement preventive policies, controls and procedures;
- identify and assess the firm's exposure to money laundering risk by, for example, undertaking a risk assessment;
- perform customer due diligence to an adequate standard depending on the risk profile of that client;
- keep appropriate records;
- monitor compliance with the AML regulations, including internal communication of policies and procedures; and
- report suspicious transactions.

Further, the Money Laundering Act requires an enhanced due diligence for transactions with high-risk countries. In addition, digital companies are required to provide payment service providers with access to infrastructure services. These include, for example, interfaces for near-field communication, which is required for cashless payments by mobile phone at physical points of sale.

Violations of anti-money laundering regulations are administrative offences and will result in fines of up to €5 million or 10 per cent of the institution's total revenue.

According to recent federal jurisdiction plans, fines of up to 10 per cent of a corporation's annual turnover for regulatory offences may be imposed. Further, corporations are to be excluded from public tenders for a term of five years if they have been fined for bribery or if a member of the executive board has been convicted of bribery. At the state level, some German federal states have already adopted an act that allows their authorities to exclude companies from public tenders if the company or its employees are associated with ABC-related behaviour.

In addition, Germany has debated for years on whether companies should be held liable under a kind of criminal law (namely, corporate sanctions law) if entities' responsible persons commit crimes or regulatory offences. The previous federal government was working on such an act but ultimately could not agree on a joint draft within the coalition. Therefore, the new law could not be passed in the German parliament during the last legislative period. Although the current (new) coalition has put the bill back on the agenda, it has once again been postponed due to its political divisiveness.

In summary, despite some differences in the material scope, it is important for fintech companies to adhere to the legal requirements of ABC and AML regulations and to create a corresponding compliance structure because the risk for the company is always the same in the event of infringement as very high fines are threatened.

Read this article on Lexology

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no specific anti-financial crime guidance for fintech companies apart from the general advice that companies should always be compliant with relevant regulations. Therefore, it is essential to have an adequate compliance system in place.

The design of the compliance system and the compliance organisation is fundamentally subject to the business judgement rule as an entrepreneurial decision. The management has to make decisions based on appropriate information, acting for the benefit of the entity. Above all, in terms of compliance, this means analysing the risks to which the company is exposed as part of its business activities and repeating that continuously and regularly. Based on the risk analysis, the management must make appropriate organisational arrangements for compliance in the company, such as:

- use of increased compliance resources in countries with a high risk of corruption;
- stricter compliance checks on public contracts;
- ongoing due diligence and monitoring;
- ongoing internal training;
- separate rules for dealing with certain occupational groups;
- clear rules; and
- where appropriate, controls for contacts with competitors.

However, institutions that are regulated by the Federal Financial Supervisory Authority should comply with all applicable anti-financial crime guidance for the financial sector.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

In 2018, Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR) came into force with direct effect across the European Union. The GDPR governs the storage, viewing, use of, manipulation and other processing by businesses of data that relates to a living individual. In summary, the GDPR requires that businesses only process personal data where that processing is done in a lawful, fair and transparent manner, as further described in the GDPR.

The GDPR requires that any processing of personal data be done pursuant to one of six lawful bases for processing. The most commonly used lawful basis for processing is to obtain the consent of the data subject to that processing – in relying on this lawful basis, the business must ensure that the consent is freely given, specific, informed and unambiguous, and capable of being withdrawn as easily as it is given. This places a significant burden on businesses to ensure that their customers are fully informed as to what their personal data

is being used for, which is a crucial change to the previous regime under which disclosure did not need to be so transparent. Other lawful bases for processing data include where that processing is necessary for the business to perform a contract it has with the data subject, or where required to comply with an obligation the business has at law (not a contractual obligation).

The GDPR further differs from the previous regime in that it places a significantly increased compliance burden on businesses, including, for example, mandatory requirements to notify regulators of data breaches, obligations to keep detailed records on processing, and requirements for most entities to appoint a data protection officer.

The GDPR does not apply to personal data that has been truly anonymised – as anonymised data cannot, by definition, be personal data. However, to ensure that GDPR does not apply to a certain data set, that data set must be truly anonymised. The GDPR itself gives limited guidance on anonymisation in Recital 26, requiring data controllers to consider a number of factors in deciding if personal data has been truly anonymised, including the costs and time required to de-anonymise, the technology available at the time to attempt de-anonymisation and further developments in technology.

When it comes to international data transfers, a two-step test must be carried out. First, the legitimacy of an international data transfer has the same requirements as a national data transfer. An international data transfer can only be legitimate if an analogous transfer within Germany was legitimate. Second, an international data transfer is only legitimate if the country to which data is to be transferred provides for reasonable data protection legislation. The transfer of data to other EEA members is permitted because those countries provide for an adequate level of data protection. In the case of a data transfer to a country outside the European Economic Area, it must be ensured that the country of destination also provides for an adequate level of protection. With regard to certain jurisdictions, the European Commission has provided decisions on the adequacy of data protection. Another way of ensuring that adequate safeguards are provided is the use of one of the model contracts approved by the European Commission (standard contractual clauses (SCCs)). Effective from 27 June 2021, the European Commission has adopted a new version of SCCs, covering various modules, taking into account the Court of Justice of the European Union decision in *Schrems II*. In addition, there is theoretically another solution that renders an assessment of the second step (legality of a data transfer to an entity in a country without an adequate level of data protection) unnecessary, namely, corporate binding rules (CBRs). CBRs are codes of conduct and a set of rules a company can draft to allow data transfer outside the European Economic Area and to overcome some practical problems with SCCs. From an EU perspective, the United States does not provide for adequate protection of personal data. If personal data is to be transferred to the United States, a Transfer Impact Assessment is required in addition to the use of the SCCs or CBRs. Depending on the risk identified, additional contractual, organisational and technical measures must be taken to establish an adequate level of data protection.

Businesses that infringe the GDPR may be subject to administrative fines of an amount up to €20 million or 4 per cent of global turnover, whichever is higher.

In Germany, the new Federal Data Protection Act came into force at the same time as the GDPR. The Federal Data Protection Act makes use of opening clauses, such as for the

Read this article on Lexology

processing of personal data in the context of employment and for the appointment of data protection officers. The oversight of the GDPR, including compliance and enforcement, is carried out in Germany by 16 data protection supervisory authorities (one supervisory authority based in each federal state). German data protection authorities have not issued any specific guidance for fintech companies.

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

'Fintech' is understood in Germany as technology-enabled innovation in financial services often resulting in new business models, applications, processes or products each materially affecting the traditional provision of financial services. Owing to the technology-neutral regulation of financial markets in Germany, there are no cybersecurity standards specifically addressing fintech companies.

The Federal Financial Supervisory Authority's (BaFin) standards on cybersecurity reflect the traditional demarcations of regulatory frameworks in Germany: the German Banking Act (namely, BaFin Circular 10/2017 on Banking Supervisory Requirements for IT), the Insurance Supervision Act (namely, BaFin Circular 10/2018 on Insurance Supervisory Requirements for IT/Supervisory Requirements for IT in Insurance Undertakings) and the German Capital Investment Code (namely, BaFin Circular 11/2019 on Capital Management Supervisory Requirements for IT/Supervisory Requirements for IT in German Asset Managers).

Regarding obligations to report serious payment security incidents under Directive (EU) 2015/2366 (revised Payment Services Directive), implemented in Germany by the German Act on the Supervision of Payment Services, BaFin has set out guidance in Circular 08/2018 (BA) for reporting serious payment security incidents (effective until 30 September 2022) and in Circular 03/2022 for reporting serious payment security incidents (effective from 1 October 2022).

According to BaFin, compliance with its sector-specific standards on IT security and cybersecurity does not relieve any regulated entity from complying with other (general) standards in this field. For Germany, this refers to standards issued by the Federal Office for Information Security (BSI), including the IT-Basic Protection Compendium, the Standards 200-1 to 200-3 (security and risk management) and the Technical Guidelines. Fintech businesses must also comply with IT and data security requirements stipulated in other applicable laws (such as the GDPR).

Certain stakeholders in the financial markets are, thus, also regulated as operators of a critical infrastructure or digital service, or both, under the German IT Security Act. Briefly, any facility or installation (or parts thereof) in the finance and insurance sectors is considered a critical infrastructure if their failure or impairment would lead to considerable supply bottlenecks or threats to public safety. Digital services are electronically provided services relating to online marketplaces, search engines and cloud-computing applications; these are likewise regulated if they qualify as 'critical' in the aforesaid meaning and provide the public with finance or insurance products. Specific guidance on identifying critical infrastructure and services in practice is provided in the form of legislative decrees of the German Federal Ministry of the Interior. Operators of critical infrastructure are, inter alia,

obliged to take appropriate organisational and technical precautions to avoid disruptions to the availability, integrity, authenticity and confidentiality of their IT systems, components or processes, as far as these are essential for the functionality of their critical infrastructure (see section 8a, paragraph 1 of the BSI Act). The same accounts for critical service providers in terms of IT security and network security (see section 8c of the BSI Act). As detailed by the BSI, both obligations require regulated entities to implement various measures to ensure network security.

BaFin is conducting regular checks relating to the IT infrastructure of regulated entities. These aspects are likewise covered in audits performed by data protection supervisory authorities. Resulting from the latest amendments of the German IT Security Act, the BSI is furnished with information and audit rights. Further, fintech businesses must comply with the IT security requirements that are stipulated in any other applicable law, such as the GDPR.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

There is a legal regime for outsourcing by financial service providers or investment firms. The Banking Act and the Securities Institutions Act set the framework and the German Federal Financial Regulatory Authority's (BaFin) Circular on Minimum Requirements for Risk Management (MaRisk) further details the requirements for outsourcing in chapter AT9. Further, BaFin indicates that the European Banking Authority's Guidelines on Outsourcing Arrangements are also relevant to BaFin's administrative practice.

In broad terms, it can be said that the outsourcer needs to ensure that its risk profile does not change owing to the outsourcing and that the outsourced services must be in compliance with the applicable legal requirements. The outsourcing of services must not lead to outsourcing of the management's responsibilities and the regulator must not be hindered in its supervisory activities owing to the outsourcing. Further, the outsourcing agreement must meet certain criteria, if material parts of the business are outsourced. Controlling and audit functions may only be outsourced to an extent that it does not bias the capability of the outsourcing entity to monitor, understand and manage the risks it incurs during its business operations.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

German regulatory law stipulates specific legal requirements relating to IT outsourcing and, as such, cloud computing in the financial services industry. Regulatory guidance is given in this context by MaRisk. According to MaRisk, any material outsourcing requires

an outsourcing agreement in writing that fulfils minimum requirements, such as stipulating audit rights (in favour of the financial services provider as well as the supervisory authority), data protection and exit management. In addition, BaFin published a Circular on 'Bank regulatory requirements relating to IT'. This guidance specifies MaRisk requirements relating to IT risk and information security management as well as the concrete IT operation, and, therefore, is also relevant to cloud computing in the financial services industry. With particular regard to the procurement of cloud services, BaFin and Deutsche Bundesbank – the German central bank – have also published 'Guidance on outsourcing to cloud service providers'. The Guidance does not contain any new requirements; the existing requirements for outsourcing, therefore, remain unchanged.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

According to German copyright law, computer programs shall be protected if they represent individual works in the sense that they are the result of the author's own intellectual creation. No other criteria, especially qualitative or aesthetic criteria, shall be applied. The protection granted shall apply to the expression in any form of a computer program. Ideas and principles underlying any element of a computer program, including the ideas and principles underlying its interfaces, shall not be protected. A copyrightable work is protected as of the moment of creation, so no further administrative measures are needed. The German Act on Copyright and Related Rights comprises specific stipulations concerning various uses of software, including decompilation and rearrangement of software. While software as such is not patent-protectable, computer-implemented inventions may be if they show a technical effect.

Business methods and software as such are not patent-eligible; both the German Patent Act and the European Patent Convention say so explicitly. However, for practical purposes, the patent eligibility of software very much depends on the claim drafting: if the invention can be presented as having a technical effect, patent protection may be available. The case law of both the Federal Court of Justice and the European Patent Office boards of appeal provide useful guidance in this respect.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

In Germany, the intellectual property generated by an employee will, generally, not automatically become the gratuitous property of the employer as in most other jurisdictions. Rather, the German Act on Employees' Inventions provides a complex system according to which the employer merely has a right to claim an employee invention. In this case, the employer

must pay a certain amount that is calculated in a complex manner based on a number of factors and parameters.

These rules do not apply to independent contractors or consultants. If the intellectual property is based on true cooperation, this can lead to complex legal situations, including the factual foundation of a private partnership. Accordingly, any such potential issues should be dealt with in a contract, clearly allocating the rights and obligations of all parties arising under such a cooperation or research and development project.

With respect to software developed by an employee, the German Act on Copyright and Related Rights contains a different set of rules. Generally, the employer will automatically gain the exclusive usage rights on software developed during employment. Only the German equivalent of moral rights will remain with the creator of such software.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Subject to contractual stipulations, co-ownership of inventions and patents as well as other intellectual property rights is considered a simple company-like structure (*Gemeinschaft*). This legal form is dealt with in the German Civil Code, though only in rudimentary form. Each owner may use the invention (as a rule, without having to pay a licence fee to the others) or may sell its share in the invention. However, a licence may only be granted with the consent of all co-owners. Each co-owner can request that the *Gemeinschaft* be dissolved, which typically happens by way of selling the intellectual property asset. This is one reason why co-owners should devise a contract early on rather than relying on statutory rights.

In addition, the German trade secret law, unlike patent and copyright law, does not regulate the legal relationship between joint owners and can, therefore, cause difficulties if no contractual provisions are established.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Germany implemented the German Trade Secrets Act almost four years ago, which chiefly protects trade secrets. In addition, trade secrets are secondarily protected under criminal law as well as through general civil law, civil procedure law and unfair competition law (against general passing-off). In addition, contracting parties are free to protect individually defined trade secrets.

The most debated criterion for gaining trade secret protection are the trade secret measures that have to be implemented by the trade secret owner. Even years after the Act came into force, there is still little clarification as to what is meant by this. There is, however, consensus that adequate protection does not require the best possible protection not to restrict the concept of secrecy too severely. The type and scope of the measures ultimately depend on the importance of the information for the company. For the sake of clarity, a

three-level classification is used. A distinction can be made between top secret (the crown jewels information, the disclosure of which would threaten the existence of the company), important (information, the disclosure of which could cause a permanent economic disadvantage) and sensitive information (information, the disclosure of which could cause a short-term economic disadvantage) (see *OLG Schleswig*, 28 August 2022, 6 U 39/21).

Further, it is important to know that the law protects trade secrets against direct unlawful attainment, use and disclosure, as well as against indirect infringement, but generally not against reverse engineering. In the event of an unlawful action, the owner of a trade secret generally has the same legal remedies available to him or her as would be the case for other intellectual property (namely, cease and desist, destruction, disclosure, damages). A special feature of the German Trade Secrets Act is a specific right to information about infringing products. Thus, it can prove a powerful tool to protect confidential information when other intellectual property rights might not be applicable.

The German Trade Secrets Act does not contain any provision as regards former employees in relation to the protection of trade secrets. Therefore, contractual provisions are advisable. Nevertheless, they must be carefully worded to be effective and not unduly limit employees' basic rights under the German Constitution.

It is at the discretion of the court to decide which orders are necessary for adequate trade secret protection during legal proceedings. The German Trade Secrets Act stipulates special regulations that apply to trade secret litigation proceedings only and prevails through execution proceedings. At the request of a party, contentious information can be fully or partly classified as a trade secret. Parties to the proceedings and individuals with access to procedural documents can neither use nor disclose trade secrets. There is no in-camera proceeding, but the number of individuals gaining access to procedural documents can be limited to one natural person from each party and their respective litigant or legal representative. In such a case the public would be excluded from the hearing when and as long as such information is discussed. The court may, at the request of one of the parties, impose a – relatively low – fine of up to €100,000 or imprisonment for up to six months for failure to comply with the obligations. The German Courts Constitution Act can also be applied as it contains, inter alia, a confidentiality obligation subject to criminal prosecution for the hearing itself.

After the proceedings, it is relevant to know that the prevailing party can request to (partly) publish the decision when it is legally binding and cannot be subject to appeals anymore. Court proceedings in trade secret cases are becoming increasingly popular. As a result, the respective German federal states have recently established special court chambers for trade secrets to facilitate the enforcement of trade secret rights.

Nevertheless, a key takeaway is that trade secrets should first be categorised and documented as such and secondly, kept secret by adequate trade secret measures so that confidential treatment is ensured and accidental disclosure is avoided.

Read this article on Lexology

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

The most obvious way to protect branding under German law would be to register either a German trademark or an EU trademark. Further, some similar rights also exist, for example, for designs, as well as to some extent usage rights and name rights specifically for a company's trade name.

Before entering a market with a designation (importantly including a trade or company name), each new market entrant should conduct due diligence on its brand. As a first step, this would include an internet search for identical designations. In a second step, the trademark registers and possibly commercial registers should be reviewed with regard to the designation, at the very least as far as identical applications are concerned. This can be done in-house but also via experienced search companies and law firms.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

There are various measures against infringements of intellectual property (IP) rights. The main goal of any action, including by way of preliminary injunction, is to stop the infringer from continuing to infringe. An injunction or preliminary injunction will achieve this aim. Apart from this, all the established IP remedies are available, including claims for damages (computed by lost profits, infringer's profits or licence analogy) and for rendering account.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

Fintech companies and the fintech sector are subject to the general competition law rules in Germany. There are no specific rules in competition law targeting the fintech sector. This means that the provisions prohibiting cartels, abuse of dominance and the merger control rules, and the general principles developed in other industries, are applied.

In January 2021, the German Act against Restraints of Competition saw a major overhaul that introduced new tools to apply competition law in digital markets. The amendment focuses on rules for Big Tech companies and therefore amends rules for the abusive behaviour of strong market players primarily directed at Google, Amazon, Facebook and Apple (GAFA). In this regard, special rules have been introduced for companies of paramount significance for competition across markets. The German Federal Cartel Office (FCO) has already used these powers in proceedings against GAFA. The FCO has the ability to intervene at an early

stage and can introduce preventive measures against strong companies in strategic positions, such as the operation of platforms, including the prohibition of self-preference of own services or impeding third companies from entering the market by processing data relevant for competition. However, depending on the market definition, these powers are not limited to the digital space but may also apply to other markets such as financial services or payment solutions. There are additional rules for relative or superior market power where a 'dependent' company can claim access to data from a company in a strong market position, which must be granted in return for adequate compensation even if such data is not otherwise marketed.

Together with the new rules on abuse of a dominant market position, the rules on merger control were updated and the national filing thresholds have been increased. Transactions are now subject to merger control if:

- the parties to the transaction achieved a combined worldwide turnover of more than €500 million;
- one of the companies concerned achieved an annual turnover of at least €50 million (previously €25 million) in Germany; and
- if another company achieved an annual turnover amounting to at least €17.5 million (previously €5 million) in Germany.

Germany has an additional merger control threshold based on the value of the consideration, which remains in place. Transactions must be notified in Germany if:

- the parties to the transaction achieved a combined worldwide turnover of more than €500 million;
- one company concerned had a turnover of more than €50 million in Germany but one of the other companies concerned, including the target, did not achieve a turnover of more than €17.5 million in Germany;
- the consideration is more than €400 million; and
- the target has been active in Germany to a significant extent.

This threshold is intended to catch highly valued start-up fintech companies even if the target company does not yet have high turnover levels. A merger case that may fall into this category was the acquisition of Tink by Visa valued at €1.8 billion. The overall increase in the thresholds will mean that fewer transactions are subject to merger control proceedings.

The financial sector has also seen enforcement actions in the past. The FCO used its competition law powers in relation to payment services. The FCO found provisions in general banking terms and conditions introduced by the banking association that prevented customers from using their personal identification numbers and account numbers in independent online payment procedures to infringe competition law to cause revisions to these general terms and also enhance new (technological) developments. This decision was upheld by the Federal Supreme Court in 2020, ruling that the restrictions on third-party payment providers were an unlawful restriction on competition. The immediate effect of the judgment is limited as Directive (EU) 2015/2366) (revised Payment Services Directive) (PSD2) requires banks to grant online financial service providers (fintech companies) access to payment and account information if the customer allows it. However, some commentators

think that the judgment heralds a broader payment service liberalisation as its reasoning can be applied to other services such as savings, investment and insurance accounts.

The FCO reviewed plans of Deutsche Kreditwirtschaft to set up a joint payment system for all payment channels and decided not to raise objections for the first stage of implementation. The project, named Xpay or DK, shall combine the current e-commerce payment methods paydirekt and giropay as well as the customer-to-customer payment system Kwitt into one system. The aim of the initiative is to offer a standard product covering various payment channels in brick-and-mortar retail (point of sale), online sales (e-commerce) and payments between private persons via apps (peer-to-peer payments). In the meantime, the FCO has also not raised objections against the further development of the giropay system in standardising the payment solution of Deutsche Kreditwirtschaft after plans for an exclusivity agreement were given up. The FCO did not challenge the centralised structure of giropay as it faces powerful competitors such as PayPal, VISA and MasterCard.

One issue that has arisen across sectors is the assessment of digital pricing tools, especially in the form of pricing algorithms, which are able to observe and evaluate a large amount of market-relevant information from competitors, customers and suppliers as well as other market conditions, thus enabling their users to react quickly with solutions adapted to each individual case to these observations (dynamic algorithm pricing). A potential competition concern that has been voiced is that pricing software may help to implement and increase the reliability of cartel agreements or that pricing software can implement hub-and-spoke practices. Innovation in the fintech field remains at the forefront of interest of regulators and the competition authority of Luxembourg initiated a market study into blockchain and economics in June 2023.

In the merger space, the FCO cleared the acquisition of ControlExpert by Allianz after an in-depth review. ControlExpert provides vehicle insurance providers, leasing companies and fleet operators with automated IT-based services to settle motor vehicle damages. In light of ControlExpert's strong market position, the FCO nevertheless examined whether its range of services would become indispensable for other vehicle insurance providers as a result of the transaction and whether, as a consequence, ControlExpert's competitors would have to expect a significant loss of customers. The FCO found that a number of competitors with strong innovative power will remain in the market and are able to offer comparable services even after Allianz has entered the market. Competitors are also increasingly using artificial intelligence to automate the process of settling car insurance claims. In such a market environment, sufficient competition is also ensured in the future and the transaction could be cleared. In 2022, the FCO cleared competing merger plans by EQT to acquire Schufa and by TeamBank to increase its shareholding in Schufa, which were procedural interesting cases as transactions which could not be completed at the same time were notified by different parties. According to public sources, EQT ultimately abandoned its acquisition plans.

The value of the consideration test has been applied to the acquisition of Honey Science Corporation by PayPal Inc. The FCO found that the transaction was notifiable as Honey Science Corporation had a significant local activity owing to its active user base despite not having turnover in excess of the then applicable threshold of €5 million. Ultimately, the transaction was cleared as the FCO found no competition concern. In particular, in relation to online payment services, various operators such as Klarna, Google Pay and Apple Pay are active on the market.

Read this article on Lexology

Section 57 of the Act on the Supervision of Payment Services, which is based on section 35 of PSD2, provides for a specific legal instrument similar to competition law that requires payment systems not to impose on payment service providers, payment service users or other payment systems any of the following: restrictive rules on the effective participation in other payment systems; rules that discriminate between authorised payment service providers or between registered payment service providers in relation to the rights, obligations and entitlements of participants; or restrictions on the basis of institutional status.

Last, the German Federal Government revised its foreign direct investment regime several times in reaction to the covid-19 pandemic. However, the overall investment regime has been amended, which applies to a variety of sectors. One particular issue is that the acquisition of companies operating a 'critical infrastructure' or a 'critical technology' is subject to a notification requirement. Acquisitions of fintech companies may become subject to a notification requirement and foreign investment if they have certain artificial intelligence capabilities or if they meet the thresholds laid down in the Regulation on Critical Infrastructure as regards payment systems.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

Since 1 January 2020, research and development activities are supported by a tax-exempt research and development allowance that will be available for all companies regardless of their size and business purposes, provided they are subject to German income tax. According to this law, in general, research and development projects are supported to the extent they can be assigned to the categories:

- basic research;
- industrial research; or
- experimental development.

According to the official reasoning of this law, the administrative practices of the European Commission regarding Regulation (EU) No. 651/2014 (General Block Exemption Regulation) as well as the Frascati Manual of the Organisation for Economic Cooperation and Development have to be considered when describing these terms.

The assessment basis for the allowance is the eligible expenses. Eligible expenses are labour costs for employees and the employer's expenditure to secure the employee's future who is entrusted with these research and development projects, including expenses for services rendered by a shareholder on the basis of an employment agreement that are subject to wage withholding tax. Further, eligible expenses are also personal contributions of an individual entrepreneur regarding these research and development projects. In this case, each labour hour is valued at €40 up to a maximum of 40 hours per week.

The assessment basis for the allowance are the eligible expenses. However, the assessment basis for the allowance is generally capped at €2 million. The research and development allowance would be 25 per cent of this assessment basis (namely, the maximum allowance is capped at €500,000 per annum). However, the assessment base for eligible expenses incurred after 30 June 2020 and before 1 July 2026 shall be a maximum of €4 million (namely, a maximum allowance of €1 million per annum applies for eligible expenses incurred after 30 June 2020 and before 1 July 2026). For contract research rendered by contractors established in an EU or EEA state, 60 per cent of the remuneration paid to the contractor is taken into account. The amount of state aid granted for a research and development project, including research allowances under this law, must not exceed €15 million per enterprise and research and development project. The allowance shall be granted on application. The application must be accompanied by an official certificate stating that research and development projects are eligible in the meaning of this law. The research and development allowance is not paid out immediately after it has been determined, but is taken into account in the next income or corporate income tax assessment by offsetting it against the determined income or corporate income tax. If the research allowance exceeds the established income or corporate income tax, the excess amount will be paid out.

Apart from this, there have, until now, been no specific tax incentives available regarding the fintech environment. However, the following should be noted.

- The German Income Tax Act allows small and medium-sized businesses (namely, taxpayers with profits of not more than €200,000 (before considering an investment deduction amount according to section 7g(1), sentence 1 of the German Income Tax Act) to deduct up to 50 per cent of the anticipated costs for future acquisitions or productions of depreciable movable fixed assets from their taxable income up to three fiscal periods before the capital asset is actually purchased. The maximum investment deduction amount is €200,000.
- Further, the German Corporate Income Tax Act, in principle, foresees that the transfer of more than 50 per cent of the shares in a German company results in an entire forfeiture of tax loss carryforwards. However, tax loss carryforwards (as well as interest carryforwards) will not be forfeited in the event of a transfer of shares beyond these thresholds if the business operation is maintained unchanged by the seller since the establishment of the company (or at least from the beginning of the third fiscal period preceding the year of the transfer) and also by the acquirer until the end of the transfer year. Even though companies in all industries are entitled to benefit from such rule according to the official reasoning of the law, this rule should serve in particular to increase the chances of IT start-ups attracting capital.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

No.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

Citizens of the European Union and the European Economic Area have unrestricted access to the German labour market. Swiss nationals also enjoy free movement within the European Union but must apply for a special declaratory Swiss residence permit.

Third-country nationals who wish to work in Germany need a residence permit that includes a work permit. There are no specific immigration schemes for fintech businesses.

However, special regulations for highly qualified employees and job positions in 'shortage occupations' apply.

A privileged residence permit exists for highly qualified persons: the EU Blue Card. The Blue Card is limited to a maximum term of four years when issued for the first time. Third-country nationals who are entitled to hold a Blue Card can obtain a national visa for entry in advance at the relevant German diplomatic mission. Only nationals of a few exempted third-country states are allowed to enter Germany without a visa for a maximum duration of three months and have the opportunity to apply for a Blue Card in Germany directly. The national visa can be replaced by a Blue Card after entry and filing a Blue Card application by the relevant immigration authority.

To obtain a Blue Card, no priority examination (no preferential workers available for the job) and no examination of working conditions are necessary (which would normally be required). The applicant needs to provide evidence of his or her qualifications, meet the labour market requirements in Germany and provide a German employment agreement with a German employer. In general, a university degree from a German university, a recognised degree from a foreign university or at least a foreign university degree comparable to a German university degree is required. A minimum salary of €58,400 gross per year (for 2023; the threshold differs annually) is required. For shortage occupations, the minimum annual gross salary is €45,552 (for 2023). Shortage occupations are, inter alia, natural scientists, mathematicians, medical doctors, engineers, engineering scientists and academic specialists in information and communication technology. If those requirements are met, no approval from the employment agency is necessary.

After a residence of 33 months in Germany, holders of a Blue Card can apply for an indefinite settlement permit. If sufficient knowledge of the German language can be proven (at least level B1), an indefinite settlement permit can already be applied for after 21 months of residence in Germany.

Skilled workers have advantages concerning their access to the German labour market. By definition of the law, skilled workers are university graduates as well as qualified workers from non-EU member countries. IT professionals who can demonstrate at least three years of professional experience do not need a formal vocational qualification. As of 1 March 2020,

all skilled workers are on an equal footing with university graduates. It is now also irrelevant whether Germans or EU citizens are available for the vacant position. This was only applicable to 'shortage professions' in the past.

In comparison to the Blue Card, the Skilled Worker Act specifies that an employment contract does not have to be issued upon arrival. Instead, one can apply for a visa for up to six months to seek a job according to one's qualifications, provided that one's foreign qualifications have been recognised and the applicant has sufficient language skills to perform the desired activity.

For applicants without a university degree who have completed professional training, a temporary residence permit can be applied for. Applicants are hereby no longer limited to positions in a shortage occupation. The applicant must provide a specific job offer, which corresponds to his or her completed training, a German qualification or a qualification recognised as equivalent, a completed professional training (of at least two years) and the applicant must provide sufficient language skills to perform the desired activity. A priority examination is not required.

Third-country citizens who come to Germany to take on a job within the same group of companies have the option to apply for an Intra-Corporate Transfer Card (ICT Card). This option includes employees working in a position as manager, specialist or trainee. To apply, a specific employment contract for the intra-corporate transfer and previous employment in the group of companies of at least six months are required. The length of stay in Germany depends on the particular type of ICT Card.

After five years of holding a preliminary residence permit, it is possible to obtain an indefinite residence permit. Proof is required that:

- the living costs can be covered without using statutory benefits;
- at least 60 months of compulsory contributions to the statutory pension insurance have been made;
- the applicant has sufficient German language skills;
- he or she has basic knowledge of the legal and social order as well as living conditions in Germany;
- a permit for employment is available;
- no threat to public safety and order by the residence; and
- sufficient housing space is available for the applicant and, as the case may be, for family members.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

The legislature and the regulatory authorities have taken unprecedented measures to address the risks deriving from the covid-19 pandemic. These measures include, inter alia, those that are specifically targeted at start-up companies and the fintech sector.

Read this article on Lexology

* *The authors wish to thank Martin Gramsch, Janine Marinello, Lena Schäfer, Elmar Weinand, Kilian Wolf and Jan Zücker for their assistance in the preparation of this chapter.*

Christopher Götz	christopher.goetz@simmons-simmons.com
Daniel Kendziur	daniel.kendziur@simmons-simmons.com
Jochen Kindermann	jochen.kindermann@simmons-simmons.com
Sascha Kuhn	sascha.kuhn@simmons-simmons.com
Sascha Morgenroth	sascha.morgenroth@simmons-simmons.com

Lehel Carre, Thierschplatz 6, Munich 80538, Germany
Tel: +49 89 20 8077 6300
www.simmons-simmons.com

Read more from this firm on Lexology

Read this article on Lexology

Greece

Alexandra Th Kondyli, Nikos Askotiris, Eleana Rouga, Maria Chronaki, Dimitris Passas, Dimitra Karampela, Anna Pechlivanidi and Sergios Charalambous*

Karatzas & Partners Law Firm

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 199

General innovation climate 199
Government and regulatory support 200

FINANCIAL REGULATION 200

Regulatory bodies 200
Regulated activities 201
Consumer lending 202
Secondary market loan trading 202
Collective investment schemes 203
Alternative investment funds 203
Peer-to-peer and marketplace lending 203
Crowdfunding 204
Invoice trading 204
Payment services 204
Open banking 205
Robo-advice 205
Insurance products 206
Credit references 206

CROSS-BORDER REGULATION 207

Passporting 207
Requirement for a local presence 207

SALES AND MARKETING 207

Restrictions 207

CRYPTOASSETS AND TOKENS 208

Distributed ledger technology 208
Cryptoassets 208
Token issuance 209

ARTIFICIAL INTELLIGENCE 209

Artificial intelligence 209

CHANGE OF CONTROL 210

Notification and consent 210

FINANCIAL CRIME 210

Read this article on Lexology

Anti-bribery and anti-money laundering procedures 210
Guidance 211

DATA PROTECTION AND CYBERSECURITY 211
Data protection 211
Cybersecurity 212

OUTSOURCING AND CLOUD COMPUTING 213
Outsourcing 213
Cloud computing 213

INTELLECTUAL PROPERTY RIGHTS 214
IP protection for software 214
IP developed by employees and contractors 214
Joint ownership 214
Trade secrets 214
Branding 215
Remedies for infringement of IP 215

COMPETITION 216
Sector-specific issues 216

TAX 216
Incentives 216
Increased tax burden 216

IMMIGRATION 217
Sector-specific schemes 217

UPDATE AND TRENDS 218
Current developments 218

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

The fintech landscape in Greece is currently growing, considering several significant investors have entered the Greek fintech and neobank industry, particularly in connection with the carve-out of the merchant acquiring business of all four Greek systemically important banks, as well as in the field of cloud-based payments. In addition, key organisations and stakeholders (including financial institutions, universities and think tanks) have created fintech hubs and clusters, to support and promote the sustainable development of Greek fintech.

New technology-friendly legislation also has been enacted, recognising and providing legal certainty on matters related, among others, to distributed ledger technology and smart contracts, as well as artificial intelligence (Law 4961/2022 on Emerging information and communication technologies, strengthening of digital governance and other provisions; the Digital Transformation Law).

Read this article on Lexology

This positive market climate, coupled with the absence of any local law peculiarities going beyond the scope of the EU financial regulatory framework, has reinforced confidence in Greece's thriving technology ecosystem and is expected to promote innovation and lead to further development of the Greek fintech sector.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Both the central bank of Greece, the Bank of Greece (BoG), and the Hellenic Capital Market Commission (HCMC) encourage financial innovation.

The BoG has established a Regulatory Sandbox, enabling participants to carry out small-scale testing of innovations, in a controlled regulatory environment, within specified parameters and timeframes, based on direct feedback and customised guidance from the regulator. The Regulatory Sandbox is aimed at facilitating innovation in Greece, through an ecosystem embracing emerging technologies, in compliance with the regulatory requirements applying to service providers. The regulatory dialogue in the context of the Regulatory Sandbox enhances legal certainty and is meant to contribute to the stability of the Greek financial system.

In addition, the BoG has created a FinTech Innovation Hub, a structure enabling the BoG to cooperate with relevant entities and provide non-binding guidance on regulatory expectations in relation to financial products, services or business models, including licensing or registration aspects of such projects. The BoG publishes the Report of its FinTech Innovation Hub on an annual basis.

The HCMC has established a Financial Innovation Hub, mainly to provide regulatory guidance to firms launching innovative financial products or services, to promote the sustainable development of fintech in Greece and to identify any need for clarification or amendment in the existing regulatory framework. The HCMC has also established a Fintech Forum that brings together academics, researchers, representatives of startup incubators or accelerators and agencies, for the dissemination of knowledge and information about the fintech industry.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

Greece follows, in principle, an institutional approach to financial supervision, in the sense that a firm's activities (for example, an entity authorised as a credit institution, an investment firm, or an insurance company) essentially determines which regulator is entrusted with its supervision, from a safety and soundness and a business conduct perspective. As such, there are no special agencies or authorities regulating or supervising fintech products and services.

Read this article on Lexology

The BoG is the competent regulatory and supervisory authority for banking, financing, payment and insurance services and products, namely:

- Credit institutions (the country's four systemic credit institutions are subject to the European Central Bank's supervision in the context of the Single Supervisory Mechanism, while less significant credit institutions continue to be subject to supervision by the Bank of Greece (BoG), subject to exceptions under EU law);
- electronic money institutions;
- payment institutions;
- leasing companies;
- factoring companies;
- credit companies;
- credit servicing firms;
- bureaux de change;
- microfinance institutions;
- insurance companies; and
- insurance distributors.

The Hellenic Capital Market Commission (HCMC) is the competent authority in relation to investment firms, crowdfunding platforms operators, asset managers (including alternative investment funds managers) and investment funds.

Fintech services falling under these broad categories are regulated and supervised by either the BoG or the HCMC.

Relevant also is the National Cybersecurity Authority, which is a General Directorate of the Ministry of Digital Governance; however, its supervisory scope is limited to systemic credit institutions.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

All of the activities listed in Annex I to Directive 2013/36/EU (CRD), as transposed by article 11 of Greek Law 4261/2014 (the Banking Law) are regulated activities that trigger licensing requirements. The same applies for services listed in Section A of Annex I of Directive 2014/65/EU on markets in financial instruments (MiFID II). More specifically, activities trigger a licensing requirement include:

- banking services (ie, taking deposits and granting credit). Credit institutions are the sole entities that are eligible under Greek law to take and hold deposits, in terms of repayable funds;
- provision of credit and loans on a professional basis;
- investment services, as found under MiFID II Annex II;
- the provision of payment services or payment-related services (third-party-providers) according to Greek Law 4537/2018 transposing Directive (EU) 2015/2366 in Greek law (the PSD2 Law). Where any service involves the issuance of e-money, a dedicated authorisation to operate as an e-money institution is required according to Law 4021/2011, which transposes Directive 2009/110/EC;

Read this article on Lexology

- leasing and factoring are also regulated and both require an authorisation under Greek law;
- credit companies and microfinance institutions (such as those eligible to offer 'buy now, pay later' services);
- operating a bureau de change (foreign currency exchange) also requires a special licence;
- operating a crowdfunding platform;
- managing claims, such as servicing NPL portfolios, require a special authorisation for a claims management company, under Greek law; and
- managing investment funds.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Greece has adopted the EU consumer protection framework. Under Greek law, a consumer is defined as any natural person acting for purposes outside the scope of their commercial, business, craft or independent professional activity.

Directive 2008/48/EC on credit agreements for consumers has been transposed into Greek law, applying to consumer credits above €200 but not exceeding €75,000. Consumer credit agreements are subject to pre-contractual and contractual information requirements (including interest rate transparency), and consumer borrowers are granted specific rights (including the right of withdrawal within 14 days of the conclusion of the credit agreement).

With respect to consumer loans relating to residential immovable property, Law 4438/2016 has transposed Directive 2014/17/EU. That law provides for precontractual information obligations, creditworthiness assessments, the valuation of real estate properties and loans denominated in foreign currencies. Mortgage credit intermediaries are regulated and subject to prior authorisation.

Consumer lending-related prudential rules are supervised by the BoG, and consumer protection rules by the Ministry of Development and Investment.

Secondary market loan trading

6 | Are there restrictions on trading loans in the secondary market in your jurisdiction?

Secondary market loan trading is regulated in Greece. In particular, the transfer of loans can take place only to specific types of entities, while there is a parallel requirement to delegate the management of receivables to a special purpose vehicle that has been licensed as servicer by the BoG. The management of the receivables (including but not limited to any loan restructuring) is exclusively performed by the servicer, the latter being in compliance with the Banking Code of Conduct, which sets guidelines for designing and evaluating viable arrears resolution solutions for borrowers. The same restrictions apply equally to all subsequent transfers of receivables.

Business receivables can be transferred by way of sale to a special purpose entity in the context of securitisation transactions in combination with the issuance and offer, by private

placement only, of bonds, the repayment of which is funded by the proceeds from the transferred business receivables or by loans, credits or financial derivative instruments. The completion of the transfer requires certain formalities, including the registration of the transfer agreement with the pertinent public record, while the special purpose entity acquiring the business receivables must observe periodic reporting obligations with the BoG and the HCMC.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

In Greece, both collective investment schemes (CIS) and the management of CISs are regulated. In general, a CIS is an investment vehicle that collects investments (funds) from the investors and creates a common pool of assets, managed collectively pursuant to a predefined investment policy.

The general regulatory regime for CIS in Greece consists of the transposition of Directive 2009/65/EU on the coordination of laws, regulations and administrative provisions relating to undertaking for collective investment in transferable securities (UCITS Directive) and Directive 2011/61/EU on Alternative Investment Fund Managers (AIFM Directive), in addition to the Greek regulatory regime that apply to specific types of CIS.

Fintech companies would not typically fall to be regulated as CIS.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Managers of alternative investment funds are regulated in Greece under the AIFM Directive, which was transposed into Greek law by Law 4209/2013 (AIFM Law).

The AIFM Law provides for the licensing requirements, internal organisational requirements, enhanced reporting and investors disclosure obligations as well as investment and leverage restrictions.

Depending on the nature of their products or services, fintech companies will be outside the scope of the AIFM Law, if their activities do not constitute an investment fund.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Peer-to-peer and marketplace lending are not specially regulated in Greece and are subject to the generally applicable regulatory provisions. The operator of a lending platform will be subject to the requirements set out in Regulation (EU) 2020/1503 (the Crowdfunding

Regulation) and to prior authorisation by the HCMC. Purchasing bonds issued in the context of a bond loan by a Greek *société anonyme* is not, in principle, a regulated activity.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

The Crowdfunding Regulation governs the provision of crowdfunding services in Greece (ie, the matching of business funding interests of investors and project owners through the use of a crowdfunding platform). Crowdfunding services can be either lending-based or investment based (ie, placing without a firm commitment basis of transferable securities and admitted instruments and the reception and transmission of client orders, for crowdfunding purposes).

The Crowdfunding Regulation provides for an EU-wide regulatory framework setting out a number of organisational and operational obligations, as well as of conduct of business rules. Pursuant to Greek Law 4920/2022, which transposes Directive (EU) 2020/1504 and implements the said Regulation, the HCMC has been designated as the national competent authority for licensing crowdfunding service providers established in Greece and for supervising them. Crowdfunding service providers authorised by the HCMC have a European passport for the provision of services in other EU member states on a cross-border basis or through a permanent establishment (branch), or both, following the completion of a simplified notification process.

In addition to the European Framework, HCMC offers a regulatory sandbox and a relevant forum to raise and discuss issues for, inter alia, firms providing or wishing to provide equity crowdfunding services. As of February 2023, the sandbox is operational.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

Pursuant to Greek Law 1905/1990, factoring, including factoring with or without recourse, the collection of receivables, the discounting of receivables and sales ledger administration are regulated activities that can be performed either by factoring companies licensed and supervised by the BoG or by banks lawfully established and operating in Greece. Factoring companies are subject to corporate governance, regulatory capital, reporting and conduct of business requirements.

Payment services

12 | Are payment services regulated in your jurisdiction?

Yes, payment services are regulated in Greece pursuant to the PSD2 Law, the relevant EU regulations and implementing regulatory provisions issued by the BoG. Only banks, payment institutions and electronic money institutions licensed by the BoG or by another EU regulator are allowed to provide payment services in Greece. All institutions entitled to provide payment services are subject to corporate governance, outsourcing and regulatory

reporting requirements, as well as to the limits on the level of interchange fees set out in Regulation (EU) 2015/751.

The PSD2 Law largely reiterates the provisions of Directive (EU) 2015/2366, including the requirements in relation to credentials and authentication, safeguarding of funds, accounting and record keeping. Payment institutions and electronic money institutions are allowed to provide payment services through an agent, following a notification to the BoG.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

The PSD2 Law regulates the following third-party payment services providers:

- aggregators and account information service providers (AISPs), in relation to the online service to provide consolidated information on one or more payment accounts; and
- payment initiation services providers (PISPs), in relation to the online initiation of orders for the transfer of funds from the payer's payment account held at another financial institution to payment accounts of merchants, which are immediately informed of the payment initiation.

The PSD2 Law does not permit to financial institutions maintaining payment accounts from denying access to the accounts they maintain, provided an AISP or PISP is authorised, the relevant payment service user has given its explicit consent and there is no suspicion of fraud. No contractual relationship needs to exist between an AISP or PISP and the account servicing financial institution. However, the scope of this prohibition is limited to payment accounts that are accessible online.

PISPs can have access to a payer's account either directly (through an adapted customer online banking interface) or indirectly (through a dedicated application programming interface).

The issuers of card-based payment instruments can also request confirmation on the availability of funds to process transactions depending on a payment by card.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Robo-advice, that is, the provision of investment advice or portfolio management services (in whole or in part) through an automated or semi-automated system, is not specifically regulated in Greek legislation. However, the supervisory expectations of the HCMC should be aligned with the relevant 'ESMA Guidelines on certain aspects of the MiFID II suitability requirements' (ESMA35-43-1163), which specify certain information requirements

applicable to providers of robo-advice (eg, explanation of the extent of human involvement and description of the sources of information used for the provision of investment services).

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Yes, fintech companies intending to sell or market insurance products in Greece must be registered with the competent Chamber as an insurance agent, an insurance broker, a coordinator of insurance agents or an ancillary insurance intermediary, and comply with relevant legislation, mainly Greek Law 4583/2018 transposing Directive (EU) 2016/97 (IDD) into Greek law (the IDD Law) and the regulatory provisions enacted by the BoG. Greek banks are, by definition, insurance agents. Insurance distributors registered in another EEA jurisdiction are also allowed to market insurance products in Greece, either on a cross-border basis or through a branch, following a notification process.

The kind of remuneration for each type of insurance distributor is defined in the IDD Law; for instance, an insurance agent is remunerated only through commissions paid by the insurers whose products are distributed, while an insurance broker is remunerated through commissions paid by the relevant insurer or fees paid by the customer and must not be legally or financially dependent on any insurer. The IDD Law contains a number of organisational, product governance and conduct of business rules applicable to distributors of insurance products (for instance, pre-contractual and contractual information requirements, or the requirement of prior advice to a customer, meaning that any insurance product sold must be consistent with the customer's insurance demands and needs, as ascertained in advance by the insurance distributor). The relevant individuals must have sufficient knowledge and ability to discharge their duties, and there are specific principles and constraints applicable to the cooperation between different insurance distributors.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

The provision of credit references or credit information services is not specifically regulated in Greece. However, the relevant framework would be the Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and the Regulation 462/2013/EU on credit rating agencies.

It is noted that an anonymous interbank company, Tiresias, operates in Greece with shareholders being the largest Greek banks. Tiresias manages a credit profile databank and specialises in the collection and supply of credit profile data on corporate entities and individuals, as well as the operation of a risk consolidation system regarding consumer credit. Additionally, Tiresias develops inter-banking information systems and provides information and communication services to all parties concerned.

Read this article on Lexology

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

EEA service providers have a European passport and can provide services through both an establishment (branch or tied agent) and on a cross-border basis to clients in Greece, after having completed a notification process initiated with their home state regulator. In contrast, non-EEA (third country) firms do not have any passport and cannot offer regulated services in Greece, unless they have established a branch or a subsidiary in Greece, which is licensed by the Bank of Greece (BoG) or the Hellenic Capital Market Commission (HCMC), as the case may be.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

There is no licence available for the provision of financial services by non-EEA firms on cross-border basis, without establishing a branch or a subsidiary. If a fintech company intends to provide a regulated service to clients in Greece, it must have been licensed by the Greek competent authorities (the BoG or the HCMC) or by the competent regulator in another EEA jurisdiction.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Selling and marketing of financial services and products in Greece will trigger the respective licensing or passporting requirements.

Sales and marketing of financial services and products are subject to the generally applicable restrictions to marketing communication, namely, false or misleading information and unsolicited communication are prohibited, and the marketing material must be presented in an easy-to-understand manner. Minimum information requirements (eg, risk disclosures), suitability checks or even requirements in relation to the professional skills of the individuals involved may also be applicable.

Services and products that fall within the Markets in Financial Instruments Directive (MiFID II) or the Banking Law framework are subject to the special marketing, minimum information and pre-contractual checks provided for by the relevant framework.

Where a customer qualifies as a consumer, additional requirements will apply under the consumer protection legislation (mainly Greek Law 2251/1994) (in relation to unfair general

terms and conditions, misleading advertising, unfair commercial practices, etc), which generally transposes the relevant EU consumer protection framework.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

The Digital Transformation Law introduces the concepts of distributed ledger technology (DLT), blockchain and smart contract in the Greek legal system, expressly recognising transactions made through such novel digital tools, making use of the blockchain technology.

A smart contract is defined as the set of encoded computer functions, which is finalised and executed through DLT technology in automated electronic form, through instructions for the 'execution' of an action, omission or tolerance, which are based on the existence or not of specific conditions, in accordance with terms recorded directly in electronic code, programmed instructions or programmed language. The terms of a smart contract may either be formulated by the contracting parties and incorporated into the code of a computer program, or be predetermined in the blockchain or other DLT and selected or accepted by the contracting parties. It also is made clear that the parties to a smart contract are considered to be bound by it from the moment of completion of their 'adherence' to it.

The Digital Transformation Law created an innovative legal framework, which provides legal certainty, by extending the scope of application of the fundamental principles of the Greek Civil Code to smart contracts. Smart contracts can facilitate and render more attractive the conclusion of different types of financial contracts, such as derivative products, however the Digital Transformation Law did not regulate specifically the use of blockchain technology by fintech companies.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

Under the AML Law and Hellenic Capital Market Commission (HCMC) decision 5/898/3.12.2020, Virtual Currency Services Providers cannot provide any service, unless they have been registered in the specific registry established by the HCMC, by providing certain information on their AML compliance policy and internal audits, their corporate and ownership status, their management and their business plan. However, such registration does not amount to any type of licensing or authorisation as a financial institution.

Apart from the above registration and generally applicable legislation regulating investment services (which may be applicable only to the limited extent that a financial instrument, eg, a derivative in the form of a smart contract, is involved) there are no rules or regulations on

the marketing and selling of cryptoassets. The PSD2 Law standards do not apply to crypto-currencies, unless and to the extent that a payment instrument is involved.

It is noteworthy that the European Parliament is in the process of approving the Markets in Crypto-Assets Regulation (the MiCA Regulation), setting harmonised rules on cryptoassets that do not constitute financial instruments (including asset-referenced tokens, electronic money tokens and utility tokens). The MiCA Regulation is expected to provide for an authorisation and passport regime for cryptoasset service providers, investor protection rules, and rules on the operation of a trading platform.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

There are no specific rules regulating the issuance and offering of tokens. To the extent a token qualifies as a transferable security within the meaning of the MiFID II Law, generally applicable financial law provisions (eg, in relation to the publication of a prospectus) will apply. However, currently there is no provision explicitly enabling the token-based issuance of equity and debt securities.

The MiCA Regulation, after its entry into force, will regulate public offerings and the placing of cryptoassets.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

Subject to general data protection rules, the Digital Transformation Law provides for certain requirements applicable to businesses using artificial intelligence systems, notably that any medium-sized or large entity must keep a register of systems used, establish and implement a policy on the ethical use of data, and inform affected employees when artificial intelligence is used for purposes related to the human resources. That Law also regulates the public procurement of services related to the design or development of artificial intelligence systems, but it does not contain any specific provision on the use of artificial intelligence by fintech companies.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Shareholders intending to hold, directly or indirectly, at least 10 per cent (a qualifying holding) in the share capital and/or voting rights of certain regulated entities (including banks, payment institutions, electronic money institutions, investment firms, alternative investment fund managers, credit servicing firms) must submit a prior notification to the Bank of Greece (BoG) or the Hellenic Capital Market Commission (HCMC) (as the case may be), which is competent to approve or oppose the acquisition.

Prior notification and approval is also required, if it has been decided to carry out an acquisition, directly or indirectly, or the further increase, directly or indirectly, of a qualifying holding, as a result of which the proportion of voting rights or capital held would reach or exceed 20 per cent, one-third or 50 per cent, and/or which would result in the target entity becoming a subsidiary of the acquirer.

For these purposes, both individual shareholdings and aggregate stakes of shareholders acting in concert must be considered.

Special notification and consent requirements apply to specially regulated entities (for example, real estate investment companies).

Notification requirements apply and, under specific circumstances, additional licensing procedures are followed vis-à-vis the competent authorities when the business that a regulated entity pursues changes, as this may impact crucial licensing requirements, such as regulatory capital, internal organisational requirements, or the requisite qualified staffing.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Greek Law 4734/2020, which transposed Directive (EU) 2018/843 (AML 5) and amended Greek Law 4557/2018 (the AML Law), extended the scope of AML customer due diligence and reporting requirements to the providers of services for the exchange between virtual and fiat currencies and custodian wallets (the virtual currency services providers) and established a register for such service providers, maintained by the Hellenic Capital Market Commission (HCMC). Virtual currencies are defined as digital representations of value that are not issued or guaranteed by a central bank or a public authority, are not necessarily attached to a legally established currency and do not possess the legal status of currency or money but are accepted by natural or legal persons as a means of exchange and can be transferred, stored and traded electronically.

Read this article on Lexology

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

No specific guidance has been issued by any Greek competent authority, apart from HCMC decision 5/898/3.12.2020 specifying the technical aspects of registration of virtual currency services providers in the relevant HCMC register.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

In Greece, there is no specific law or guidance relating fintech companies use of personal data.

The processing and transfer of personal data are generally governed by the General Data Protection Regulation (GDPR) and the following local laws:

- Law 4624/2019 on the personal data protection authority, implementing the GDPR and transposing Directive 2016/680/EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
- Law 3471/2006 on the protection of personal data and privacy in the Electronic telecommunications sector, which transposed the Directive 2002/58/EU on Privacy and electronic communications; and
- Law 2472/1997 on the protection of individuals with regard to the processing of personal data, which transposed the Directive 95/56/EU (now defunct except for explicit provisions in article 84 of Law 4624/2019 implementing the GDPR into domestic legal order).

According to the GDPR, in order for any processing of personal data to be lawful must be done in accordance with the following principles:

- the data subject has given consent to the processing for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests

or fundamental rights and freedoms of the data subject that require protection of personal data.

Regarding anonymisation, according to recital 26 of the GDPR, where the data has been processed in such a way that it is truly anonymous (ie, information that does not relate to an identified or identifiable natural person or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable), the principles under GDPR do not apply to the processing of this data.

With respect to any transfers of personal data to third countries or international organisations, the general rule under the GDPR is that transfers may only take place to a non-EU country if European Commission has decided that the third country, a territory or one or more specified sectors within that third country ensures an adequate level of protection. In the absence of such decision, the transfer may only take place if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available or if the requirements of article 49 GDPR are met (derogations for specific situations).

In Greece, the Hellenic Data Protection Authority is responsible for compliance with the European and Greek data protection rules.

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

Greek Law 4577/2018, which transposes EU Directive 2016/1148/EU, concerning measures for a high common level of security of network and information systems, sets out general cybersecurity requirements for infrastructures and relevant service providers (eg, risk identification and management, adoption of technical security measures, incident reporting). However its scope is limited, based on implementing regulatory provisions, to the Greek systemically important banks.

Specific cybersecurity requirements are also provided for in sector-specific legislation, such as the PSD2 framework or the Banking Law. The Bank of Greece (BoG) has adopted, through Executive Committee Act No. 190/2/16.6.2021, the relevant EBA Guidelines on ICT and security risk management, as well as EBA Guidelines on major incident reporting, through BoG Executive Committee Act No. 209/3/19.07.2022, respectively. These apply to the whole range of financial Institutions, save for investment firms.

It is also noteworthy that the Hellenic Cybersecurity Authority has issued a handbook and a self-assessment tool to indicate good practices (not specifically for the financial sector), which are not legally binding.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

The outsourcing of critical or important functions (such as those that are necessary for the soundness, continuity and regulatory compliance of core business activities, or those that may impact the effectiveness the internal control functions) by a regulated entity is subject to regulatory constraints, subject to ongoing supervision by the Bank of Greece (BoG) or the Hellenic Capital Market Commission (HCMC), as the case may be. The outsourcing must not result in the delegation by senior management of its responsibility, and the relationship and obligations of the outsourcing firm vis-à-vis its clients must not be altered.

Depending on the type of the financial institution and the scope of the envisaged outsourcing, an outsourcing arrangement may be subject to certain minimum content requirements (including, for instance, the agreed service levels, safeguards ensuring that the outsourcing entity effectively monitors the outsourced functions and can terminate the arrangement with immediate effect (where necessary), or having in place an exit plan clarifying the consequences of termination). The BoG and the HCMC have certain information rights in relation to outsourcing arrangements, which may be subject to prior notification to the regulator and to record-keeping requirements. Outsourcing to service providers located in third countries (ie, other than an EEA member state) is generally subject to even stricter requirements; for instance, the MiFID2 regime (Commission Delegated Regulation (EU) 2017/565) provides that an appropriate cooperation agreement should be in place between the competent authority of the outsourcer and the supervisory authority of the service provider.

Moreover, pursuant to the BoG's Executive Committee Act 190/2/16.06.2021 transposing the EBA Guidelines on Information and Communications Technology (ICT) and Security Risk Management (EBA/GL/2019/04), regulated entities (such as banks, payment institutions, electronic money institutions, micro-credit institutions and credit companies) entering into an agreement with a third-party provider of information and communications technology (ICT) services and ICT systems, must specify in such agreement certain issues, such as data and network security, data encryption, security monitoring processes or incident handling procedures.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

Arrangements for outsourcing to cloud service providers are subject to certain regulatory requirements. In particular, the BoG has adopted the EBA Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03) through Executive Committee Act 178/5/2.10.2020, and the HCMC has also endorsed the ESMA Guidelines on outsourcing to cloud service providers (ESMA50-164-4285).

Read this article on Lexology

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

In Greece, software may be protected either as copyright pursuant to the rules of Greek copyright law (Law 2121/1993) or as patent pursuant to the rules of Greek patent Law (Law 1733/1987). In Greece, there are no registration proceedings for copyright protection. To obtain a patent on a software, a patent application shall be submitted before the Greek competent authority (ie, the Hellenic Industrial Property Organization) and relevant filing fees shall be paid.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

According to the Greek copyright law (Law 2121/1993), all exploitation (economic) powers on all copyrightable works (including software) developed by an employee during the course of employment are automatically transferred to the employer (in the Greek usual practice, employment contracts include in any case an IP transfer clause in favor of the employer). If the IP has been developed by contractors or consultants, there is no automatic transfer of IP rights; however, a separate written agreement should be concluded with the creator (contractor or consultant) for the execution of the IP rights' transfer.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Under the Greek copyright legislation, the creators of a work, which is the product of collaboration, are the original co-beneficiaries of the (economic) powers and moral rights on the copyrighted work. Unless otherwise agreed, the IP rights belong equally to both co-creators or joint owners. Therefore, both joint owners have the right to use and exploit their IP. Unless otherwise agreed, a licence, charge or an assignment to the IP may be made if joint owners mutually agree.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

In Greece, trade secrets (including confidential information) are protected according to the provisions of Law 1733/1987 (as applicable following the enactment of Law 4605/2019). Under these rules, the acquisition of a trade secret is considered legal when the trade secret comes from an independent discovery or creation. In the case of infringement of a

trade secret, injunctive relief may be sought and if requested by the injured party, the court shall order the infringer, who knew or should have known that he was unlawfully acquiring, using or disclosing a trade secret, to pay the trade secret owner damages equivalent to the actual loss suffered as a result of the unlawful acquisition, use or disclosure.

In relation to court proceedings, according to Greek legislation, any person who participates in legal proceedings concerning the illegal acquisition, use or disclosure of a trade secret, or who has access to documents that are part of said legal proceedings procedures, is prohibited from using or disclosing any trade secret. Also, under the requirements of the legislation, the court may, at the request of a party, take special measures necessary to protect the confidentiality of any trade secret.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

In Greece, for the interested party to protect branding, it usually applies for a trademark pursuant to the provisions of the Greek trademark Law 4679/2020. To obtain a trademark right, the interested party should file a trademark application before the Greek competent authority (ie, the Hellenic Industrial Property Organization) requesting the registration of a trademark. The trademark is protected for 10 years from the filing date and may be renewed upon payment of the required renewal fees.

Fintech businesses may ensure that they do not infringe existing brands if, before applying for a trademark registration, they conduct a pre-check on the available information on the existing trademark databases (including the EUIPO's trademark database).

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

Individuals or companies whose intellectual property rights have been infringed may seek injunctive relief requesting the immediate prohibition of the infringement and compensation. In the case of copyright and trademark infringement, administrative fines (in the case of illegal distribution of computer programs or audio hardware) may be imposed and criminal penalties may also be imposed (for the illegal reproduction of copyrighted material or products illegally bearing third party's trademarks).

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

There are no such specific competition issues.

In December 2022, the Hellenic Competition Commission published a fintech sectoral study, which points out that the Greek fintech market is new and still under development, and that currently there is no remarkable finding as regards cryptocurrencies or wealth and asset management or personal finance management. That said, the study stresses the need to monitor potential self-preferencing or enveloping practices and identifies certain entrance barriers to the payment infrastructure or systems market, mainly, due to the applicable regulatory constraints. It also states that the lack of interoperability of application programming interfaces, as there are no formalised technical standards, may provoke inequalities in the open banking market between incumbents and new entrants regarding client data processing.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

There are no specific tax incentives available for fintech companies and the investors in Greece.

However, in Greece there are some general tax incentives to which financial technology companies and investors, among others, can be subject. For instance, research and development costs, including the depreciation of equipment used for scientific and technological research, are deducted from the gross revenue of companies at the time of their realisation, increased by 100 per cent.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

There are no specific new or proposed tax laws or guidance that would significantly increase tax or administrative costs for fintech companies in Greece.

However, fintech companies should monitor developments in the tax laws and regulations in Greece, as the tax landscape is constantly evolving and new tax laws and guidance may be introduced in the future.

Read this article on Lexology

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

There are no specific immigration schemes for international staff of fintech companies.

Citizens of member states of the EU, the EEA and of the Swiss Confederation (workers, self-employed persons and their family members) have the right to move and reside freely in Greece, subject to a registration requirement, when they intend to reside for a period exceeding three months, in accordance with the Greek Presidential Decree 106/2007.

Nationals of third countries (ie, other than EU, EEA and Swiss citizens) need a residence permit. Apart from the ordinary process, there are three more procedures that can be followed to recruit skilled staff from a third country. More specifically, a third-country national wishing to be employed in a highly skilled position can apply for the EU Blue Card. The basic requirements are the conclusion of an employment contract of at least one year with a legal entity in Greece for the provision of highly specialised services with a minimum annual wage of about €32,000 and proof of high professional qualifications. According to the newly voted immigration legislation, which will apply from 1 January 2024, the minimum duration of the employment contract will be six months, and the salary should be at least equal to eight-fifths of the average gross annual salary in Greece.

In exceptional cases, when strategic investments are taking place in Greece, a more flexible and faster procedure for the administration of residence permits is available. This route presupposes a prior recommendation by the competent public authority describing the reasons for public interest and quoting the details of employees who are nationals of third countries and need to move in Greece for the purpose of the investment. This kind of residence permit is issued for a period of up to two years and may be renewed for an equal period. With effect from 1 January 2024, its duration is increased to three years.

Finally, in the case of intercorporate transfers of directors and skilled employees, the ordinary process is followed, subject to the following specific features: an intercorporate connection between the companies involved, the employee's (or director's) previous experience of at least 12 consecutive months in the company and the experience in and specialist knowledge of relevant entity's activity, techniques and management. The duration of this residence permit cannot exceed three years. However, after the expiry of such a permit, the employee can apply for an EU Blue Card.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

The 2020 Digital Finance Package is expected to be added to the regulatory framework applicable to the participants in the Greek fintech market. As Regulation (EU) 2022/858 (DLT Pilot Regime Regulation) has already entered into force (in a way complementing the Bank of Greece's regulatory sandbox and allowing the experimentation with a new, more efficient financial market architecture), the much-anticipated adoption of Markets in Crypto-Assets Regulation will also help ease legal uncertainty for both regulators and market participants, regarding the use and circulation of cryptoassets and stable coins, as both investments and as means for executing payments.

At the same time, the impact of the Digital and Operational Resilience Act (Regulation), published in December 2022 but applicable only in early 2025, regarding the compliance cost to financial institutions is not yet clear. On the upside, however, fintech institutions may always benefit from a proportional to their size application of the requirements set therein, becoming, at the same time, less prone to operational risks deriving from information and communications technology disruptions, while enjoying the associated reputational benefits.

* *The authors wish to thank Dimitra Karampela, Anna Pechlivanidi and Sergios Charalambous for their assistance in the preparation of this chapter.*

KARATZAS & PARTNERS

Alexandra Th Kondyli	a.kondyli@karatza-partners.gr
Nikos Askotiris	n.askotiris@karatza-partners.gr
Eleana Rouga	e.rouga@karatza-partners.gr
Maria Chronaki	m.chronaki@karatza-partners.gr
Dimitris Passas	d.passas@karatza-partners.gr
Dimitra Karampela	d.karampela@karatza-partners.gr
Anna Pechlivanidi	a.pechlivanidi@karatza-partners.gr
Sergios Charalambous	s.charalambous@karatza-partners.gr

The Orbit-5th floor, 115 Kifissias Ave, Athens 115 24, Greece
Tel: +30 210 371 3600
www.karatza-partners.gr

Read more from this firm on Lexology

Read this article on Lexology

Hong Kong

Jolyon Ellwood-Russell, Michelle Ta, Donia Chu and Galvin Chua

Simmons & Simmons

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 220

General innovation climate 220
Government and regulatory support 221

FINANCIAL REGULATION 222

Regulatory bodies 222
Regulated activities 222
Consumer lending 224
Secondary market loan trading 224
Collective investment schemes 225
Alternative investment funds 225
Peer-to-peer and marketplace lending 226
Crowdfunding 226
Invoice trading 226
Payment services 226
Open banking 227
Robo-advice 227
Insurance products 228
Credit references 228

CROSS-BORDER REGULATION 229

Passporting 229
Requirement for a local presence 229

SALES AND MARKETING 229

Restrictions 229

CRYPTOASSETS AND TOKENS 229

Distributed ledger technology 229
Cryptoassets 230
Token issuance 231

ARTIFICIAL INTELLIGENCE 231

Artificial intelligence 231

CHANGE OF CONTROL 232

Notification and consent 232

Read this article on Lexology

FINANCIAL CRIME 232
Anti-bribery and anti-money laundering procedures 232
Guidance 233

DATA PROTECTION AND CYBERSECURITY 233
Data protection 233
Cybersecurity 234

OUTSOURCING AND CLOUD COMPUTING 235
Outsourcing 235
Cloud computing 235

INTELLECTUAL PROPERTY RIGHTS 236
IP protection for software 236
IP developed by employees and contractors 237
Joint ownership 237
Trade secrets 238
Branding 238
Remedies for infringement of IP 238

COMPETITION 239
Sector-specific issues 239

TAX 239
Incentives 239
Increased tax burden 239

IMMIGRATION 239
Sector-specific schemes 239

UPDATE AND TRENDS 240
Current developments 240

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Hong Kong is home to more than 800 fintech companies and start-ups, covering services in the areas of payment, artificial intelligence, wealthtech, blockchain and insurtech. As is fitting for an international financial centre, more than one-third of fintech founders are from other countries. Nearly half of the established fintech companies have been in operation for more than three years. Consumer fintech adoption is high and consumers have a significant desire for financial products and services, although business-to-business services remain the biggest driver of fintech development in Hong Kong. The Hong Kong government supports the sector and has strengthened cooperation with regulators in other jurisdictions to encourage cross-border fintech development.

In 2019, the Hong Kong Monetary Authority (HKMA) granted eight 'virtual bank' licences to new entities, all of which have launched online-only banking services. A number of licence

holders have now begun developing, testing and launching new products in credit, loans, wealth and insurance.

Hong Kong's regulators continue to examine the fintech sector and to evolve their approach on regulatory changes and sector initiatives. The Securities and Futures Commission (SFC) and the HKMA reviewed their approach on regulation for virtual asset-related activities of intermediaries and the SFC and HKMA jointly issued a revised guidance on this in January 2022 (replacing the 2018 guidance). In October 2022, the SFC set out in a circular the requirements under which the SFC would consider authorising exchange-traded funds that obtain exposure to virtual assets primarily through futures contracts for public offering in Hong Kong.

In June 2022, the Hong Kong government gazetted the Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022, which sets out the new licensing regime that any person who seeks to carry on a business of operating a virtual asset exchange is required to apply for an SFC licence. The Bill was passed by the Legislative Council of Hong Kong in December 2022 and will take effect on 1 June 2023. The SFC has issued a consultation paper on the proposed regulatory requirements for SFC-licensed virtual asset trading platform operators in Hong Kong in February 2023, with the aim of obtaining market feedback on the implementation of such licensing regime.

The HKMA's Fintech 2025 strategy is to drive fintech development in Hong Kong and includes the agenda of encouraging all banks to fully digitalise front-end and back-end operations, exploring the use of central bank digital currencies, creating data infrastructure (including a commercial data interchange, digital corporate identity and blockchain-based credit data sharing platform) and nurturing fintech talent – in turn with the aim of building an overall appetite for fintech solutions in Hong Kong.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Fintech is identified by the Hong Kong government as a priority investment area.

A range of Hong Kong government funding support programmes are also available to research and development of fintechs, including the Enterprise Support Scheme (ESS) and Partnership Research Programme and the R&D Cash Rebate Scheme, as well as scale-up support such as the HK$2 billion Innovation and Technology Venture Fund, SME Financing Guarantee Scheme and Technology Voucher Programme (among others).

The SFC operates a Fintech Contact Point and the HKMA established a Fintech Facilitation Office, which, in each case, is intended to facilitate the fintech community's understanding of the current regulatory regime and for the regulators to work with market participants to support the sustainable development of the fintech industry, including the Fintech Supervisory Sandbox established by the HKMA and the Regulatory Sandbox established by the SFC that permits new and existing licensed entities to carry out regulated activities within a confined regulatory environment prior to launching on a wider scale.

The HKMA is one of the founding contributors of, and the SFC has joined as a coordination group member of, the Global Financial Innovation Network. The SFC has also signed cooperation agreements with a number of overseas regulators, including the UK's Financial Conduct Authority and the Australian Securities and Investments Commission. Pursuant to these agreements, the SFC will cooperate to share information on emerging fintech trends, developments and related regulatory issues, as well as on organisations that promote innovation in financial services.

In September 2017, the Insurance Authority launched a fast-track scheme to expedite applications by insurance companies using solely digital distribution channels as a means to promote the development of insurtech in Hong Kong, with one virtual bank offering insurance via its virtual banking platform since 2021.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

The main regulatory bodies are the Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC) and the Insurance Authority.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Pursuant to the Securities and Futures Ordinance, the following activities are regulated and trigger a licensing requirement:

- Type 1: dealing in securities;
- Type 2: dealing in futures contracts;
- Type 3: leveraged foreign exchange trading;
- Type 4: advising on securities;
- Type 5: advising on futures contracts;
- Type 6: advising on corporate finance;
- Type 7: providing automated trading services;
- Type 8: securities margin financing;
- Type 9: asset management;
- Type 10: providing credit rating services;
- Type 11: dealing in OTC derivative products or advising on OTC derivative products (not yet in operation but is included under the Securities and Futures Ordinance); and
- Type 12: providing client clearing services for OTC derivative transactions.

For the purposes of the above categories, 'securities' are very widely defined and include stocks, shares, loan stock, bonds, debentures, all rights and interests in such securities, interests in collective investment schemes and structured products. However, shares and debentures of a private Hong Kong company do not constitute securities. Hong Kong private companies are companies incorporated in Hong Kong that restrict members' rights to

Read this article on Lexology

transfer shares, limit the maximum number of shareholders to 50 and prohibit the making of an invitation to the public to subscribe for shares or debentures.

The licensing regime applies irrespective of whether the specified activities take place in Hong Kong or, if a person is actively marketing these activities to the public in Hong Kong, from outside Hong Kong.

The activities that are most relevant to fintech businesses are likely to be dealing in securities and advising on securities. Dealing in securities includes making or offering to make an agreement with a person, or inducing or attempting to induce another person to enter into an agreement to acquire, dispose, subscribe or underwrite securities. Advising on securities includes giving advice on whether, and the terms on which, securities should be acquired or disposed of and issuing analyses or reports for the purpose of facilitating decisions on whether to acquire or dispose of securities. It is also possible that some fintech platforms could constitute automated trading services, the operation of which requires a licence.

In addition to the above licensing requirements, if a business is undertaking banking activities, such as receiving money on a current, deposit, savings or similar account or paying or collecting cheques, such a business is required to be licensed as a bank by the HKMA.

Certain other activities, such as moneylending, money exchange services, money remittance services and money broking services, also require licences from the HKMA or the Commissioner of Customs and Excise.

The operation of stored value facilities (such as prepay cards or prepay mobile apps) or designated retail payment systems is subject to a licensing regime under the Payment Systems and Stored Value Facilities Ordinance and requires a licence from the HKMA.

A new licensing regime for virtual asset trading platform operators has recently been introduced and will come into effect on 1 June 2023. The Hong Kong government gazetted the Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022, which introduced the new licensing regime, and the Bill was passed by the Legislative Council of Hong Kong in December 2022. From 1 June 2023, any centralised virtual asset trading platform operator carrying on their businesses in Hong Kong or that actively markets its service to Hong Kong investors without a valid licence will commit a breach under the new Anti-Money Laundering and Counter-Terrorist Financing Ordinance irrespective of whether they provide trading services in security tokens, unless they qualify for a 12-month transition period. A platform operator that is in operation in Hong Kong immediately prior to 1 June 2023 and has a 'meaningful and substantial presence in Hong Kong' may be eligible for the transitional arrangements. The SFC has issued a consultation paper on the proposed regulatory requirements for SFC-licensed virtual asset trading platform operators in Hong Kong in February 2023 to obtain market feedback on the implementation of the licensing regime – consultation conclusions remain pending as at the date of writing this article.

Read this article on Lexology

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Under Hong Kong law, the offering and provision of consumer lending is not distinguished from primary lending.

Lending (consumer lending and primary lending) is a regulated activity in the jurisdiction and is governed by the Money Lenders Ordinance. The Money Lenders Ordinance requires that all loans made available in Hong Kong are by licensed moneylenders or authorised institutions (eg, licensed banks, restricted-licence banks and deposit-taking companies under the Banking Ordinance).

There are a number of exemptions that, if applicable, mean no formal licence is required. The loan and lending entity would need to satisfy one of the specified categories of exempted lenders and exempted loans in Schedule 1 of the Money Lenders Ordinance. Examples of exempted loans are:

- a loan made bona fide for the purchase of immovable property on the security of a mortgage of that property;
- a loan made bona fide to refinance such a mortgage;
- a loan made by a company, firm or individual whose ordinary business does not primarily or mainly involve the lending of money in the ordinary course of that business;
- an intra-group loan; and
- a loan made to a company that has a paid-up share capital of not less than HK$1 million or an equivalent amount in any other approved currency.

The Money Lenders Ordinance prohibits the adoption of excessive interest rates. With effect from 30 December 2022, the statutory interest rate cap for lending is lowered from 60 per cent to 48 per cent per annum. Lending at an interest rate beyond 48 per cent per annum constitutes an offence and the relevant loan agreement is not enforceable. The threshold of the extortionate rate is also lowered from 48 per cent to 36 per cent per annum. Lending at an interest rate beyond 36 per cent per annum is presumed to be extortionate and may trigger the reopening of the relevant transaction by the courts.

Secondary market loan trading

6 | Are there restrictions on trading loans in the secondary market in your jurisdiction?

Secondary market loan trading is not a regulated activity in itself but it constitutes primary lending regardless of whether the loan has been fully drawn and, therefore, the loan and lender are subject to the restrictions of the Money Lenders Ordinance.

However, secondary market loan intermediation is not a regulated activity, provided that it does not involve any lending or deposit-taking and provided that loans are not in the form of securities.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Broadly, a scheme is a collective investment scheme under Hong Kong law if it has the following four elements:

- it is an arrangement in respect of property;
- participants do not have day-to-day control over the management of the property even if they have the right to be consulted or to give directions about the management of the property;
- the property is managed as a whole by or on behalf of the person operating the arrangements or the contributions of the participants, or both, and the profits or income from which payments are made to them are pooled; and
- the purpose of the arrangement is for participants to participate in or receive profits, income or other returns from the acquisition or management of the property.

A collective investment scheme can cover any property and that property does not need to be located in Hong Kong for the scheme to be a collective investment scheme. 'Property' in this context is not limited to real property.

It is an offence in Hong Kong to issue any marketing material that contains an offer to the Hong Kong public to acquire an interest or participate in a collective investment scheme unless it has been authorised by the SFC or an exemption applies. Promoting a collective investment scheme may also constitute a regulated activity for which a licence is required. It is possible that certain fintech activity could constitute a collective investment scheme where the business concerned is managing assets on behalf of participants who have invested through a fintech platform (eg, investing in real estate or debt securities). Careful analysis of the specific circumstances and the way in which the platform permits investors to participate will be required to determine whether it constitutes a collective investment scheme.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Management of securities or futures contracts or real estate investment schemes constitutes a regulated activity as it falls under Type 9: asset management of the Securities and Futures Ordinance. Accordingly, managers of alternative investment funds that invest in real estate or securities (which are widely defined) or futures contracts require a licence to do so.

The SFC has confirmed that companies engaged in the distribution to the Hong Kong public of funds that invest in virtual assets are required to be licensed for Type 1 activity whether or not such virtual assets amount to 'securities'. In addition, the SFC will now apply additional conditions on licensed corporations that manage or distribute funds that invest, solely or partially (more than 10 per cent of the gross asset value) in, or that have a stated investment objective to invest in, virtual assets. These conditions include a restriction that such funds can only be invested in, or offered to, professional investors.

Read this article on Lexology

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

There are no specific regulations applicable to peer-to-peer (P2P) or marketplace lending in Hong Kong. The SFC has issued a notice reminding potential P2P businesses that activity such as P2P lending might constitute a regulated activity, but much will depend on the precise structure of the platform. For example, it is likely that a platform offering debentures or loan stocks would constitute a regulated activity of dealing in securities.

Additionally, it is an offence in Hong Kong to issue any marketing material that contains an offer to the Hong Kong public to enter into an agreement to acquire or dispose of securities, unless an exemption applies.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

There are no specific regulations concerning crowdfunding. However, certain crowdfunding activity is likely to constitute a regulated activity. For example, equity crowdfunding is likely to constitute dealing in securities and possibly advising on securities, both of which are regulated activities in Hong Kong. As such, the operator of these platforms would need to be licensed by the SFC.

Additionally, it is an offence in Hong Kong to issue any marketing material that contains an offer to the Hong Kong public to enter into an agreement to acquire or dispose of securities unless an exemption applies.

Invoice trading

11 Describe any specific regulation of invoice trading in your jurisdiction.

To the extent that an invoice is purchased, without risk of being re-characterised as a loan for the purposes of the Money Lenders Ordinance, with true sale there is no specific regulation on the buying and selling of invoices. This is common in factoring and invoice discounting arrangements.

However, if invoices are opened to the public and crowdfunded then the operator of the trading platform needs to follow certain regulations. It is usually the case that if a platform investor is classed as a professional investor, then much of the regulation around crowdfunded invoicing might not apply, depending on the platform structure.

Payment services

12 Are payment services regulated in your jurisdiction?

Payment services include a wide range of activities such as taking cash deposits, making cash withdrawals, executing payment transactions, issuing or acquiring payment instruments,

issuing and administering means of payment, making payments sent through the intermediary of a telecoms, IT system or network operator, or even providing stored value cards or devices.

Payment services are regulated activities in Hong Kong and are subject to the Banking Ordinance, the Anti-Money Laundering and Counter-Terrorist Financing Ordinance and the Payment Systems and Stored Value Facilities Ordinance (as applicable).

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

The HKMA published the Open Application Programming Interface (Open API) Framework for the Hong Kong Banking Sector in July 2018, which encourages financial institutions to make information available through Open APIs within a staged time frame depending on the type of information but this is not a regulatory requirement. According to the HKMA, as of February 2023, of the 28 participating banks, 24 retail banks and 20 banks with corporate and SME offerings have launched Phase III (comprising deposit account availability, status, balance and transaction details). 26 out of the 28 participating banks have launched Phase IV (comprising faster payment services app-to-app payments).

The Commercial Data Interchange (CDI) was launched in October 2022 as a new data strategy of the HKMA. The CDI enables a secure and efficient data flow between banks and sources of commercial data and is part of HKMA's Fintech 2025 strategy to improve Hong Kong's data infrastructure. Since its launch, banks have been able to access the Commercial Credit Reference Agency database via the CDI. In February 2023, the HKMA also issued a circular encouraging banks to leverage the CDI for the digitalisation of the banking process.

In relation to the use and sharing of consumer credit data, under the Multiple Credit Reference Agencies (MCRA) model, all consumer credit providers are required to connect to the Hong Kong Credit Reference Platform (CRP), which facilitates the transmission of consumer credit information in an encrypted form between the participating credit providers (such as banks and money lenders) and the credit reference agencies. This promotes a level-playing field and facilitates the development of fintech in Hong Kong in line with HKMA's Fintech 2025 strategy. The HKMA issued a revised supervisory policy manual on consumer credit data in this regard in late 2022.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Robo-advisers will require a licence from the SFC as they usually include the provision of investment advice and services for dealing in securities governed by the Securities and Futures Ordinance.

In July 2019, the SFC issued the Guidelines on Online Distribution and Advisory Platforms (the Guidelines). The Guidelines set out requirements through the application of core principles concerning the proper design of the platform, clear disclosure of information, risk management, governance, capabilities and resources, review and monitoring of activities on the platform and record-keeping. Specific guidance is also given concerning robo-advisers in respect of client profiling, system design and development, supervision and testing of algorithms and technology and staff resource requirements.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Yes, both insurance companies and insurance intermediaries (such as agents) need to be authorised or registered, or both, with the Insurance Authority in Hong Kong under the Insurance Ordinance.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

The provision of credit ratings (opinions regarding the creditworthiness of entities other than an individual, securities and agreements to provide credit) is regulated under the Securities and Futures Ordinance as a Type 10 regulated activity, but the gathering, collating, dissemination or distribution of information concerning the indebtedness or credit history of any person is not regulated by any dedicated legislation (except under data protection law); instead, consumer credit data is subject to industry codes of practice issued by the Hong Kong Privacy Commissioner together with HKMA supervisory requirements.

Against a major data breach incident of the sole consumer credit reference agency in Hong Kong in 2018, the Hong Kong government commenced a review of this area, and as a result, the Hong Kong CRP launched in November 2022. Under the MCRA model, all consumer credit providers are required to connect to the CRP, which facilitates the transmission of consumer credit information in an encrypted form between the participating credit providers (such as banks and money lenders) and the credit reference agencies that promotes a level-playing field and facilitates the development of fintech in Hong Kong in line with the Fintech 2025 strategy. The HKMA issued a revised supervisory policy manual on consumer credit data in late 2022.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

No. There are no arrangements in place that enable a financial services provider to conduct any regulated activity in Hong Kong without directly holding the relevant licence for the regulated activity, or by operating through a licensed financial institution.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

It is unlikely that the Securities and Futures Commission would grant a licence for regulated activities to an entity that did not have a local presence. Equally, the Hong Kong Monetary Authority is unlikely to provide a banking licence to an entity that does not have a presence in Hong Kong as it would be difficult to see how such an entity could comply with the obligations to which it would be subject as a bank.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

The issuance of any marketing materials that contain an offer to the Hong Kong public to enter into an agreement to acquire or dispose of securities must be authorised by the Securities and Futures Commission, unless an exemption applies.

The active marketing (whether from within or outside Hong Kong) to the public in Hong Kong of activities that constitute regulated financial services in Hong Kong is prohibited unless carried out by an entity that holds a licence to carry out such services in Hong Kong.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

There are no specific regulations or guidelines regarding the use of distributed ledger technologies.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

In respect of common 'digital currencies', such as bitcoin, the Hong Kong government considers that these are virtual assets and do not qualify as digital currencies with regard to their nature and circulation in Hong Kong. In this regard, Hong Kong does not currently have any specific regulatory measures in respect of the use of virtual assets, but the existing laws provide for protection against unlawful activities in general (eg, anti-money laundering, fraud and terrorist financing).

In relation to virtual asset exchanges, the Hong Kong government gazetted the Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022, which introduces a new licensing regime for virtual asset trading platform operators. The Bill sets out that any person who seeks to carry on a business of operating a virtual asset exchange (including cryptocurrencies) is required to apply for a Securities and Futures Commission (SFC) licence, and was passed by the Legislative Council in Hong Kong in December 2022. Under the Bill, virtual asset trading platform operators would also have to carry out customer due diligence in respect of anyone trading on the exchange. The new licensing and anti-money laundering regime will take effect on 1 June 2023.

Financial institutions dealing with virtual assets are required to comply with regulations from time to time by the relevant financial regulators, the Hong Kong Monetary Authority and the Securities and Futures Commission. Additional requirements apply to companies engaged in distribution of funds that invest in virtual assets and intermediaries that carry out virtual asset-related activities.

The active marketing and sale or trading of cryptoassets that constitute securities as defined under the Securities and Futures Ordinance (which include derivatives or futures contracts relating to non-securities virtual assets such as bitcoin) is a regulated activity and requires a licence.

Further, the Hong Kong Monetary Authority (HKMA), in its consultation conclusions to the discussion paper on crypto-assets and stablecoins in January 2023 (Consultation Conclusions), proposed to bring certain activities relating to stablecoins into the HKMA's regulatory perimeter, to help address the potential financial stability risks posed by stablecoins and to promote the orderly and sustainable development of the industry. The HKMA indicated that in drawing up the specific regulatory arrangements, they will consider industry feedback, the latest market developments and international discussions, with the aim to implement regulatory arrangements in 2023–2024. The Consultation Conclusions set out the key parameters of the proposed regime, including the regulatory scope and key regulatory requirements. As there may be some potential overlaps between the HKMA's proposed regulatory arrangements and the SFC's licensing regime for virtual asset trading platform operators, fintechs should keep a close eye on developments as to how the Hong Kong regulators will approach any potential regulatory overlap.

Read this article on Lexology

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

The regulation of tokens issued in STOs, ICOs or otherwise depends on the nature of the tokens offered.

Utility tokens that only provide membership or access to a service or payment tokens that are only used as a means of payment for goods or services (such as bitcoin) are not regulated.

However, tokens that comprise securities under Hong Kong regulations (in particular, under the Securities and Futures Ordinance) are regulated. For example, tokens that represent an asset such as a debt or a claim on the issuer's assets (such as a share in future earnings) or that amount to a collective investment scheme are securities. Where the tokens being issued fall within the definition of securities, issuing, dealing in or advising on these tokens, or managing or marketing a fund investing in them, may constitute a regulated activity. Persons engaging in a regulated activity targeting the Hong Kong public are required to be licensed by or registered with the SFC, irrespective of where they are located. In addition, investment products linked to any tokens (whether securities or not), such as futures or derivatives, are considered to be securities and offering, trading or advising on these products is a regulated activity.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

The provision of investment advice is a regulated activity irrespective of the method of delivery of the advice. There are no specific regulations governing the use of artificial intelligence and the provision of robo-advice. However, the Securities and Futures Commission (SFC) has issued the Guidelines on Online Distribution and Advisory Platforms. The guidelines identify six core principles that must be complied with by operators of online advice platforms and provide additional requirements for robo-advisers.

The Hong Kong Monetary Authority (HKMA) has also issued guidance on the use of artificial intelligence in its circular on High-level Principles on Artificial Intelligence, which sets out 12 high-level principles that should be complied with by banks in a manner proportionate to the nature of the artificial intelligence application and the level of risk, as well as guiding principles on Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence. In April 2022, the HKMA also published the 'Regtech Adoption Practice Guide – Issue #6: Artificial Intelligence-based Regtech Solutions', which among other things, provides practical implementation guidance to banks on the adoption of artificial intelligence-based Regtech solutions.

Read this article on Lexology

The Hong Kong Privacy Commissioner has also issued the Guidance on the Ethical Development and Use of Artificial Intelligence, which facilitates the development and use of artificial intelligence in Hong Kong and assists organisations in complying with the provisions of the Personal Data (Privacy) Ordinance in the process of doing so.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Different consent requirements apply to the acquisition of different types of regulated businesses. In general, where a person is to become a holder of a specified percentage of a regulated entity or will control a specified percentage of voting rights of that entity, prior consent must be obtained from the relevant regulatory authority. For banks or entities that hold a licence for regulated activity, before a person acquires a holding of more than 10 per cent of the issued shares, or prior to them controlling, alone or with other associates, more than 10 per cent of the voting rights in the bank or regulated entity, consent must be sought from the Hong Kong Monetary Authority or Securities and Futures Commission respectively. Additional rules apply to persons becoming majority holders of banks and to the acquisition of indirect shareholdings in regulated entities. For corporations holding a money service operator's licence, prior approval from the Commissioner of Customs and Excise is required under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance before any person can become an ultimate owner (generally defined to mean an individual who directly or indirectly owns or controls more than 25 per cent of the issued share capital of the corporation) of the corporate licensee. Failure to obtain consent is a criminal offence. In all cases, advice should be sought as to the applicable requirements and the process for obtaining consent.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

If the relevant entity is licensed for regulated activities, is licensed as a bank, operates a money service or provides trust or company incorporation services, it needs to comply with the Hong Kong legislation in relation to anti-money laundering and counter-terrorist financing, including establishing policies and procedures to identify clients and combat money laundering and terrorist financing.

For virtual asset trading platform operators, the Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022 was gazetted by the Hong Kong government (and passed by the Legislative Council of Hong Kong in December 2022) to enhance Hong Kong's regulatory regime for combating money laundering and terrorist financing. The new

regime sets out that any person who seeks to carry on the business of operating a virtual asset exchange (including cryptocurrencies) is required to apply for a Securities and Futures Commission licence, and that such virtual asset trading platform operator would also be subject to obligations of carrying out customer due diligence in respect of anyone trading on the exchange. The new licensing regime together with the anti-money laundering obligations will come into effect on 1 June 2023.

The Hong Kong legislation in relation to the prevention of bribery would also apply, and licensed companies should have in place policies and procedures to prevent bribery.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no specific guidance for fintech companies, but there is guidance for licensed corporations and banks that would apply to fintech businesses that are licensed accordingly.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

There are no specific regulations governing the processing and transfer of data relating to fintech products and services in Hong Kong, but fintech companies are required to comply with the Personal Data (Privacy) Ordinance (PDPO) when collecting or using the personal data of individuals. Personal data is information that relates to a living person and can be used to identify that person, where the data is in a form in which access or processing is practicable. Organisations that collect and use personal data must comply with, among other things, six data protection principles, which include the following:

- personal data can only be collected for a purpose directly related to a function and activity of the data user in a lawful and fair manner, and the amount of data to be collected must not be excessive. Data subjects have to be informed of the purpose of the collection of data and how it will be used;
- data users must take all practicable steps to ensure personal data remains accurate and is deleted after the purpose of collecting this data is fulfilled;
- unless the data subject has given prior consent, personal data can only be used for the purpose for which it was originally collected or a directly related purpose;
- data users must take all practicable steps to ensure that personal data is protected against unauthorised or accidental accessing, processing, loss or erasure;
- data users should stipulate, publish and implement policies in relation to personal data that can generally be achieved by having a data privacy policy in place; and
- individuals have rights of access to and correction of their personal data. Data users should comply with data access or data correction requests within the requisite time limit, unless reasons for rejection prescribed in the PDPO are applicable.

The Hong Kong Privacy Commissioner issued an information leaflet – 'Tips for Using Fintech' – in March 2019 explaining the privacy implications and risks of fintech applications. The publication also recommends good practices in relation to data privacy for fintech operators.

The Hong Kong Privacy Commissioner has also published an information leaflet – 'Matching Procedure: Some Common Questions' – that emphasises the importance of obtaining consent from all individual data subjects or the Privacy Commissioner if the process of aggregation of personal data for commercial gain constitutes a matching procedure under the PDPO, to ensure that the risk of potential harm to the relevant data subjects is minimised. It also issued the 'Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry' and a circular to banks in 2019 on consumer protection in the use of big data analytics and artificial intelligence, which specify high-level principles of accountability, fairness, transparency and data protection.

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

There are no cybersecurity regulations or standards specifically addressing fintech businesses in Hong Kong. Cybersecurity is covered under various laws and regulations, such as the Personal Data Privacy Ordinance and the Crimes Ordinance.

The Hong Kong Monetary Authority's (HKMA) Supervisory Policy Manual sets out the key regulatory standards that the HKMA expects authorised institutions to follow in relation to technology security and has issued a number of requirements and circulars on cybersecurity risk management in recent years, requiring industry players to establish appropriate governance frameworks. Several frameworks were launched by HKMA to strengthen cyber resilience in the banking sector, including the Cybersecurity Fortification Initiative and Cyber Resilience Assessment Framework, as well as the HKMA's supervisory policy manual chapter on e-banking (TM-E-1 Risk Management of E-banking), which is of particular relevance to the virtual bank licensee.

The Securities and Futures Commission has issued the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading, and the Circular to All Licensed Corporations on Cybersecurity, setting out areas that licensed corporations should pay close attention to when reviewing and mitigating their cybersecurity risks, as well as certain controls that these corporations should consider implementing where applicable.

The Insurance Authority has issued the Guideline on Cybersecurity, which sets the minimum standard for cybersecurity that authorised insurers are expected to have in place and the guiding principles in assessing the effectiveness of an insurer's cybersecurity framework.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

The Securities and Futures Commission (SFC) has endorsed the Principles on Outsourcing of Financial Services for Market Intermediaries published by the International Organisation of Securities Commission (the IOSCO Principles) but there are no specific regulations or guidance issued by the SFC on outsourcing. There are specific requirements that regulated entities must comply with, such as record-keeping requirements, which are relevant to decisions to outsource parts of the business.

The Hong Kong Monetary Authority (HKMA), which regulates authorised institutions, such as banks, includes in its supervisory policy manual a chapter on outsourcing. The HKMA expects authorised institutions to be aware of their legal obligations to meet the minimum authorisation criteria under the Banking Ordinance in relation to outsourcing plans. In particular, authorised institutions need to have adequate accounting systems and systems of control and to conduct their business with integrity, competence and in a manner not detrimental to the interests of depositors.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

The Hong Kong Privacy Commissioner, the HKMA and the SFC have published guidelines on outsourcing and data privacy in connection with cloud computing.

The Hong Kong Privacy Commissioner has published various guidelines, circulars and information leaflets providing guidance on measures and best-recommended practices that are pertinent to cloud services. These include having contractual arrangements between providers and customers of cloud services, to address the Privacy Commissioner's key concerns relating to loss of control, and the use, retention or erasure and security, of personal data when it is stored in the cloud.

The HKMA's Supervisory Policy Manual sets out the key regulatory standards that the HKMA expects authorised institutions to follow, or else be prepared to justify non-compliance, for managing technology risks and cybersecurity, covering topics such as:

- IT governance and oversight, system development and change management;
- information processing;
- communication network management; and
- management of technology service providers.

The SFC has endorsed the IOSCO Principles in relation to 'licensed corporations' outsourcing their activities. The SFC also issued guidelines that require licensed corporations to establish

policies and procedures to ensure the integrity, security, availability, reliability and thoroughness of all information relevant to the licensed corporation's business, which extends to situations where data is stored in the cloud. Other best-recommended practices relevant to cloud computing include:

- reviewing policies and procedures to manage, identify and assess cybersecurity threats and IT security controls;
- considering the cybersecurity controls of third-party service providers; and
- ensuring continuity of critical activities and systems.

In 2019, the SFC issued a circular on the use of external electronic data storage by licensed corporations. The circular sets out various requirements in relation to licensed corporations' use of external data storage providers (EDSPs). These include requirements to obtain undertakings from EDSPs in favour of the SFC in certain circumstances and requirements regarding the management of risks and security with regard to the use of EDSPs. The SFC has also issued guidance in the form of FAQs as to how similar requirements are to apply to the use of electronic data storage provided by intragroup affiliates.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Computer programs (and preparatory design materials for computer programs) are protected by copyright as literary works under the Copyright Ordinance. Copyright arises automatically as soon as the computer program is recorded. Registration of copyright is not required and is not possible in Hong Kong.

If the software code has been kept confidential, it may also be protected as confidential information. No registration is required.

Programs for computers, and schemes, rules or methods of doing business 'as such', are expressly excluded from patentability under the Patents Ordinance.

Notwithstanding these exclusions, it is possible to obtain patents for computer programs and business methods if it can be shown that the underlying invention makes a 'technical contribution' over and above that provided by the computer program or business method itself, such as an improvement in the working of the computer. Accordingly, a well-drafted patent may be able to bring a computer-based software or business method invention within this requirement, but this may be difficult to do and will not always be possible. Registration formalities must be followed to obtain protection.

In particular, 'standard' patents are based on patents applied for and granted by one of three designated patent offices, namely, in China, the United Kingdom and the European Patent Office (where the United Kingdom is designated). They have a maximum period of protection of 20 years from the filing date of the designated application.

Read this article on Lexology

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Copyright created by an employee in the course of his or her employment is automatically owned by the employer unless otherwise agreed as provided under the Copyright Ordinance.

An invention made by an employee belongs to the employer if it was made in the course of:

- the normal duties of the employee or in the course of duties falling outside his or her normal duties, but specifically assigned to him or her, and the circumstances, in either case, were such that an invention might reasonably be expected to result from the carrying out of his or her duties; or
- the duties of the employee and, at the time of making the invention, because of the nature of his or her duties and the particular responsibilities arising from the nature of his or her duties, he or she had a special obligation to further the interests of the employer's undertaking.

Copyright or inventions created by contractors or consultants in the course of their duties are owned by the contractor or consultant unless otherwise agreed in writing. However, the person who commissions a copyrighted work has an exclusive licence to exploit the commissioned work for all purposes that could reasonably have been contemplated by the author and the person who commissioned the work at the time the work was commissioned, and the power to restrain any exploitation of the commissioned work for any purpose against which he or she could reasonably take objection.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

If copyright is jointly owned (eg, copyright in respect of a computer program that has been co-written by two people) then all joint owners must consent to any act restricted by copyright (such as its use, licensing and assignment) under the Copyright Ordinance. As a result, the commercialisation of jointly owned copyright can be a challenge unless all owners consent to its use. It is advisable for the joint owners to enter into an agreement setting out how these rights should be exercised.

In respect of patents, each co-owner is entitled to an equal undivided share in the patent and can do anything in respect of the invention for his or her own benefit without the consent or need to account to the other under the Patents Ordinance (in each case, subject to any other agreement reached between the co-owners).

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Confidential information can be protected against misuse, provided the information in question has the necessary quality of confidence, is subject to an express or implied duty of confidence, and that no registration is necessary (or possible).

Confidential information can be kept confidential during civil proceedings with the permission of the court.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brands can be protected as registered trademarks in Hong Kong. A brand can also be protected under the common law tort of passing off if it has acquired sufficient goodwill. Certain branding, such as logos and stylised marks, can also be protected by design rights and may also be protected by copyright as artistic works.

The HK Registry trademark database can be searched to identify potentially problematic trademarks that have been registered or applied for. It is highly advisable for fintech businesses to conduct trademark searches to check whether earlier registrations exist that are identical or similar to their proposed brand names. It may also be advisable to conduct searches on the internet for any unregistered trademark rights that may prevent the use of the proposed mark.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

Remedies include:

- preliminary and final injunctions;
- damages or an account of profits;
- delivery up or destruction of infringing products;
- disclosure orders; and
- costs.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

There is a competition regime under the Competition Ordinance in Hong Kong that applies to all entities carrying out business in Hong Kong. There are no particular aspects of this regime that would affect fintech businesses disproportionately to other businesses.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

There are no specific tax incentives applicable to fintech companies.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

No.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

The Hong Kong government launched different schemes to recruit skilled staff in areas including the technology and financial sectors.

The Talent List of Hong Kong was promulgated to attract people around the world who specialise in the 13 professions most needed for Hong Kong's economic development, including 'Experienced professionals in Fintech', 'Experienced data scientists and cyber security specialists' and 'Innovation and technology experts'. These candidates are potentially eligible for immigration via the Quality Migrant Admission Scheme, which does not require them to have secured an offer of local employment for settlement in Hong Kong.

The Innovation and Technology Commission introduced and launched the Technology Talent Admission Scheme in 2018, a scheme that provides a fast-track arrangement for admission

of overseas and mainland research and development talent. Eligible technology companies and institutes, including those engaged in the areas of fintech, artificial intelligence and cybersecurity, may be granted quotas to sponsor eligible persons to apply for employment visas or entry permits. In December 2022, the Innovation and Technology Commission further introduced enhancement measures to the scheme, which lifted the local employment requirement, extended the quota validity period and expanded the coverage to more emerging technology areas.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

During FinTech Week 2022, the Hong Kong government and regulators – the Hong Kong Monetary Authority (HKMA) and the Securities and Futures Commission (SFC) – signalled their sentiment to embrace fintech adoption, digital ledger technology and their applications (including in the areas of cryptocurrencies, non-fungible tokens and metaverses). Hand in hand with this, regulators emphasised the importance of creating a robust and balanced legal and regulatory framework to maintain public trust and the overarching guiding principle of 'same activity, same risks, same regulation'. The regulators also encouraged the financial sector in Hong Kong to adopt a radical open-mindedness to fintech innovation.

The Hong Kong government has introduced legislation to regulate cryptocurrency exchanges and virtual asset trading platform operators, which is due to come into effect on 1 June 2023.

The HKMA, in its consultation conclusions to the discussion paper on crypto-assets and stablecoins in January 2023 (Consultation Conclusions), proposed to bring certain activities relating to stablecoins into the regulatory perimeter. The HKMA expects to implement the regulatory arrangements in 2023–2024.

In October 2022, the SFC also announced in a circular regarding the requirements under which the SFC would consider authorising exchange-traded funds that obtain exposure to virtual assets primarily through futures contracts for public offering in Hong Kong.

The HKMA also expressed, in April 2023, encouragement for banks to support the Tiered Account Services initiative (which was introduced in 2019) and to facilitate the ease of offering banking services to small and medium-sized enterprises and start-ups (which has long been one of the more difficult tasks in setting up new businesses in Hong Kong).

The HKMA has been seeking to explore the use of central bank digital currencies to ease cross-border trade settlement, in particular the testing of e-renminbi and e-Hong Kong dollar. The HKMA issued a discussion paper to gather feedback on the feasibility of a retail e-Hong Kong dollar in April 2022 and a policy stance on e-Hong Kong dollar outlining its next steps in September 2022.

The Hong Kong government has sought to establish qualifications and competency standards for the fintech sector. It was announced in the Hong Kong government's 2022–2023

budget that the development of recognised professional qualification standards for sector practitioners under the Qualifications Framework for Fintech was underway.

Jolyon Ellwood-Russel	jolyon.ellwood-russell@simmons-simmons.com
Donia Chu	donia.chu@simmons-simmons.com
Michelle Ta	michelle.ta@simmons-simmons.com
Galvin Chua	galvin.chua@simmons-simmons.com

30th Floor One Taikoo Place, 979 King's Road, Hong Kong, Hong Kong
Tel: +852 2868 1131
www.simmons-simmons.com

Read more from this firm on Lexology

Read this article on Lexology

India

Probir Roy Chowdhury, Yajas Setlur, Kumarmanglam Vijay, Pratish Kumar and Nikhil George

JSA

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 243

General innovation climate 243
Government and regulatory support 244

FINANCIAL REGULATION 245

Regulatory bodies 245
Regulated activities 245
Consumer lending 245
Secondary market loan trading 247
Collective investment schemes 247
Alternative investment funds 248
Peer-to-peer and marketplace lending 248
Crowdfunding 248
Invoice trading 249
Payment services 249
Open banking 250
Robo-advice 250
Insurance products 251
Credit references 251

CROSS-BORDER REGULATION 252

Passporting 252
Requirement for a local presence 252

SALES AND MARKETING 252

Restrictions 252

CRYPTOASSETS AND TOKENS 253

Distributed ledger technology 253
Cryptoassets 253
Token issuance 253

ARTIFICIAL INTELLIGENCE 254

Artificial intelligence 254

CHANGE OF CONTROL 254

Notification and consent 254

FINANCIAL CRIME 255

Read this article on Lexology

Anti-bribery and anti-money laundering procedures 255
Guidance 256

DATA PROTECTION AND CYBERSECURITY 256
Data protection 256
Cybersecurity 257

OUTSOURCING AND CLOUD COMPUTING 257
Outsourcing 257
Cloud computing 258

INTELLECTUAL PROPERTY RIGHTS 259
IP protection for software 259
IP developed by employees and contractors 259
Joint ownership 259
Trade secrets 260
Branding 260
Remedies for infringement of IP 260

COMPETITION 261
Sector-specific issues 261

TAX 261
Incentives 261
Increased tax burden 262

IMMIGRATION 263
Sector-specific schemes 263

UPDATE AND TRENDS 263
Current developments 263

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

India is one of the fastest-growing fintech markets in the world with a wide range of constantly innovating and evolving sub-segments, including payments, cryptocurrency, digital banking, embedded finance, open banking, digital lending, personal finance management, and wealth, insurance and regulatory technology.

While some types of fintech are extensively regulated (such as those operating payment systems), others (such as those in the cryptocurrency space) operate in regulatory limbo.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Programmes

The Reserve Bank of India (RBI) has set up the Reserve Bank Innovation Hub (RBIH) to promote and facilitate an environment that accelerates innovation across the financial sector. The RBIH has also signed a memorandum of understanding (MoU) with certain entities to promote fintech innovation. Some notable partnerships include:

- an MoU with IIT Madras Incubation Cell to provide incubation support and nurture early-stage start-ups and empower them to transform India's fintech landscape; and
- an MoU with the India Post Payments Bank for innovations in financial products and services.

RBI has also launched HaRBInger – a global hackathon – with a view to encourage and promote fintech innovation. The theme for the 2023 edition is inclusive digital services.

The National Payments Corporation of India also plays a pivotal role in fintech innovation through its txn-nxt platform.

Regulatory sandboxes

The RBI has introduced regulatory sandboxes for testing new innovations in a controlled environment. So far, these sandboxes have been on retail payments, cross-border payments and micro, small and medium enterprise (MSME) lending and prevention and mitigation of financial fraud. As part of the fifth cohort of regulatory sandboxes, the RBI maintained a neutral theme and invited applications for innovative products, services and technologies cutting across various functions in the RBI's regulatory domain. Similarly, the Insurance Regulatory and Development Authority of India and the Securities and Exchange Board of India have also set up regulatory sandboxes for innovation in the insurance sector and the securities market ecosystem, respectively.

Incentives

The International Financial Services Centres Authority has announced its fintech incentive scheme through which monetary grants are proposed to be given to fintech companies to support their activities.

Arrangements with foreign regulators

The RBI is a member of the Global Financial Innovation Network, a network that will enable innovative firms to interact with regulators, helping them navigate between countries as they look to scale new ideas.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

India does not have a single regulator for all fintech products and services. While most areas of fintech (such as payments, digital banking and digital lending) are regulated by the Reserve Bank of India (RBI), fintech products and services that relate to insurance and securities are regulated by the Insurance Regulatory and Development Authority of India (IRDAI) and the Securities and Exchange Board of India (SEBI), respectively.

Notably, the Ministry of Electronics and Information Technology also acts as the nodal ministry to oversee all IT and internet-related products, services, developments and policies.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Licensing requirements depend on the specific sectoral regulator's regulations.

Under the SEBI, activities such as securities broking and investment advising trigger licensing requirements under the SEBI (Stock Brokers) Regulations 1992 and the SEBI (Investment Advisers) Regulations 2013 (the IA Regulations), respectively.

Under the IRDAI, insurance web aggregators, brokers and agents are required to be licensed under the IRDAI (Insurance Web Aggregators) Regulations 2017, the IRDAI (Insurance Brokers) Regulations 2018 and the IRDAI (Registration of Corporate Agents) Regulations 2015, respectively.

Under the RBI, all non-bank payment systems operators (PSOs) are required to seek authorisation from the RBI under the Payment and Settlement Systems Act 2007 (PSSA) before commencing operations. Examples of PSOs include payment aggregators, prepaid payment instrument (PPI) issuers and card networks. These PSOs are subject to additional regulations, circulars and directions issued by the RBI under the PSSA. For instance, payment aggregators are governed by the Guidelines on Regulation of Payment Aggregators and Payment Gateways and PPI issuers are governed by the Master Directions on Prepaid Payment Instruments 2021.

The RBI also requires non-bank lenders and factors to seek authorisation as non-banking financial companies (NBFCs).

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Yes. The main entities engaged in consumer lending are commercial banks and NBFCs. The RBI is the regulator with jurisdiction over these entities and their consumer lending businesses. Entities in this sector are broadly regulated under the Reserve Bank of India Act

1934 and the Banking Regulation Act 1949, as well as the various circulars, directions and regulations issued by the RBI under these laws. This body of law governs various aspects of consumer lending, including know-your-customer and anti-money laundering requirements, fair practices and procedures, and prudential norms applicable to lenders.

The RBI has also notified the Guidelines on Digital Lending (DL Guidelines) to specifically regulate digital lending, based on the report of a working group on digital lending.

The DL Guidelines apply to lending which largely uses digital technology. They primarily govern RBI-regulated entities such as banks and NBFCs. However, they also indirectly impose obligations on lending service providers (LSPs), who act as agents of regulated entities and perform some of the lender's functions on their behalf, as well as digital lending applications (DLAs), which are mobile or web-based applications facilitating digital lending.

Some obligations imposed by the DL Guidelines include:

- Disclosure-related obligations: the DL Guidelines require regulated entities to disclose all loan-related details in a key fact statement. This statement should include information such as the annual percentage rate (the annual cost of the loan), the recovery mechanism, cooling-off period, and other relevant details.
- Data-related obligations: the DL Guidelines specify that LSPs and DLAs can only store a minimal amount of personal data necessary to fulfil their obligations. This may include the customer's name, contact details and address. However, regulated entities bear the ultimate responsibility for ensuring the privacy of such data. The guidelines also impose data localisation requirements, meaning that all data collected as part of the digital lending process must be stored within India. Further, all regulated entities, DLAs and LSPs are required to have a comprehensive privacy policy in place, which aligns with the RBI guidelines and other legal requirements.
- Grievance redressal: the DL Guidelines mandate that every regulated entity and LSP interacting with customers must establish an effective grievance redressal mechanism to resolve customer disputes. They are also required to appoint grievance redressal officers and prominently display their contact details on their website and key fact statement.
- Fund flow: the DL Guidelines stipulate that all loan amounts (including repayments) must be directly disbursed from the regulated entity's account to the borrower's account. The involvement of any third-party pass-through account or pool account is expressly prohibited. That said, an exemption is granted in the case of advance salaries. In those cases, the employer is permitted to repay the loan by debiting the borrower's bank account.

Overall, the DL Guidelines aim to regulate digital lending activities, ensuring transparency, privacy protection, and fair practices for customers.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

Assignment of loan exposures of a financial institution to another financial institution or for securitisation is regulated by the RBI. All on-balance sheet exposures that are in the nature of loans and advances, and are standard (ie, performing without default) – except specified prohibited exposures – are allowed to be assigned or securitised in accordance with the applicable guidelines. The sale of non-performing assets (which are in default) is regulated by the RBI.

Assignment of loan exposures is primarily governed by Master Direction – RBI (Transfer of Loan Exposures) Directions 2021. Securitisation of standard assets in India is primarily governed by Master Direction – RBI (Securitisation of Standard Assets) Directions 2021(Securitisation MD).

Notably, the securitisation of non-performing loan assets is governed by the Master Direction – RBI (Securitisation of Standard Assets) Directions 2021, in addition to:

- the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act 2002; and
- the Securitisation Companies and Reconstruction Companies (Reserve Bank) Guidelines and Directions 2003.

Separately, the SEBI (Issue and Listing of Securitised Debt Instruments and Security Receipts) Regulations 2008 will apply if the securitisation papers or instruments are listed.

In addition, the DL Guidelines clarify that for first loan default guarantee (a mechanism under which a third party takes up the risk exposure of the loan portfolio of the regulated lender), regulated entities must adhere to the Securitisation MD.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Collective investment schemes in India are regulated by the SEBI under the SEBI (Collective Investment Scheme) Regulations 1999 and ordinarily require registration. For a scheme or arrangement to be considered a collective investment scheme, it must satisfy the following conditions:

- payments or contributions made by investors are pooled and utilised for the purpose of the scheme or arrangement;
- such contributions are made by the investors with a view to receive returns in the form of profits, income, produce or property from such a scheme;
- the property or contribution forming part of the scheme is managed on behalf of the investors; and

- the investors do not have day-to-day control over the management and operation of the scheme or arrangement.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Alternative investment funds (AIFs) are regulated by the SEBI. All AIFs are required to register with the SEBI under the SEBI (Alternative Investment Funds) Regulations 2012 (the AIF Regulations).

AIFs are broadly classified into three categories, depending on the nature of their investments. Category I AIFs invest in start-ups and early-stage ventures that are considered socially or economically desirable by the Indian government (and would include venture capital funds). Category II AIFs include funds that do not fall under Category I, but do not undertake leverage or borrowing (and would include private equity funds). Finally, Category III AIFs are funds that employ diverse or complex trading strategies and employ leverage through investment in derivatives (and would include hedge funds and private investment in public equity funds).

The AIF Regulations describe in detail the ongoing forms of compliance and requirements applicable to AIFs, including the minimum corpus for each AIF scheme, the minimum ticket size of an investor in the scheme and the minimum continuing interest or investment by the manager of the fund.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Peer-to-peer (P2P) lending platforms can only be operated by NBFCs that have obtained specific authorisation from the RBI (NBFC-P2Ps) under its Master Directions on Peer to Peer Lending Platforms 2017. The role of NBFC-P2Ps is restricted to that of an intermediary providing a platform to retail lenders and borrowers. They are also required to abide by prudential norms prescribed by the RBI and to put in place board-approved policies regarding the eligibility criteria of participants, operations, fair practice, IT frameworks, data security and business continuity.

The RBI requires fund transfers between lenders and borrowers to be facilitated only through escrow accounts operated by a bank-promoted trustee. No cash transactions are permitted.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

Equity-based crowdfunding

Funds are raised by a business by offering a share in its equity in return for investments. There is presently no specific legal or regulatory framework governing equity-based

crowdfunding. In response to notices issued by the SEBI, several popular crowdfunding platforms have applied to the regulator to register themselves as AIFs.

Reward-based crowdfunding

In consideration for their contributions, contributors receive an existing or a future tangible reward, such as early access to products or exclusive merchandise, among other things. Such crowdfunding is not prohibited or specifically regulated in India.

Donation crowdfunding

Here, funds are donated without any expectation of anything in return. Such donations could be for a social cause or artistic purposes, among others, and are not generally prohibited in India. However, foreign donations will need to comply with the provisions of the Foreign Contribution (Regulation) Act 2010.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

In India, invoice trading (factoring) is undertaken by specified NBFCs and banks. To commence the factoring business, an NBFC has to obtain a certificate of registration from the RBI. With a view to simplifying discounting for trade receivables of micro, small and medium enterprises (MSMEs), the RBI has introduced the Trade Receivables Discounting System (TReDS) Scheme, which provides for the establishment of online platforms on which MSMEs can discount their invoices drawn on to banks and NBFC factors. There are three such platforms currently licensed to operate by the RBI:

- the Receivables Exchange of India;
- the M1xchange; and
- Invoicemart.

Regulations have also been issued by the International Financial Services Centres Authority, which regulates the Gujarat International Finance Tec-city in relation to online factoring platforms.

Payment services

12 | Are payment services regulated in your jurisdiction?

Broadly, payment systems are regulated by the PSSA and the regulations made thereunder. Under the PSSA, no person can commence or operate a payment system in India without prior authorisation from the RBI. The following payment systems are regulated by the RBI:

- electronic fund transfers;
- prepaid payment instruments;
- the centralised electronic clearing system;
- point of sale terminals and online transactions using credit, debit or prepaid cards issued by card payment networks;

- paper-based payment systems such as cheque truncation, cash payments, automated teller machines (ATMs) and white label ATMs;
- mobile banking services;
- the Bharat Bill Payment System;
- the TReDS Scheme; and
- payment aggregators and payment gateways.

The RBI has issued different directions and circulars to each of the above prescribing authorisation requirements, minimum net worth and codes of conduct, among others.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

The RBI, through its Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions 2016, has come up with an open banking initiative by enabling intermediaries (account aggregators) to consolidate and share the financial information of a given customer held with different financial entities.

Account aggregators are NBFCs that have received authorisation from the RBI to undertake account aggregation. They act as a bridge between financial information providers (such as banks, banking companies, NBFCs and asset management companies) and financial information users (entities registered with and regulated by any financial sector regulator). Information flow, in this case, takes place through appropriate APIs and is subject to the explicit consent of the customer to whom the information relates.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Robo-advice is not specifically regulated by the SEBI. However, all investment advisers are required to be registered with the SEBI under the IA Regulations. In its consultation papers on the IA Regulations, the SEBI has clarified that the use of automated advice tools by registered investment advisers is not expressly prohibited. However, at present, the SEBI's requirement for physical agreements between investment advisers and clients has made it difficult for investment advisers to provide robo-adviser services.

Notably, the SEBI has also discussed the possibility of amendments to the IA Regulations to require robo-advising investment advisers to comply with audit, disclosure and targeting requirements. However, no such amendment has taken place to date.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Fintech companies engaged in the sale or marketing of insurance products are regulated by the IRDAI.

Fintech companies that operate websites to act as intermediaries between insurance companies and prospective policy buyers by collecting, compiling and comparing various policies are called web aggregators. Web aggregators must obtain a certificate of registration from the IRDAI and comply with the IRDAI (Insurance Web Aggregators) Regulations 2017.

Every insurer or insurance broker (also required to be licensed by the IRDAI) that markets insurance products must adopt fair, honest and transparent practices while issuing advertisements and avoid practices that tend to impair the confidence of the public. Such advertisements must prominently disclose the registered name of the entity.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

In India, credit information can be obtained from credit information companies (CICs), which are independent third-party agencies that collect the financial data of individuals pertaining to their loans, credit cards and other related information, and share it with their members. CICs are regulated by the RBI under the Credit Information Companies (Regulation) Act 2005 (the CIC Act), and the rules and regulations made thereunder.

CICs are permitted to reveal credit information only to specified users, which include credit institutions, certain entities regulated by the IRDAI and the SEBI, and telecom companies. Notably, credit information can also be provided to entities that process such information for the support or benefit of credit institutions, provided that they satisfy the following criteria:

- the entity should be a company incorporated in India;
- the memorandum of association of the entity should allow the business of processing of information for the benefit of credit institutions;
- the entity should have a net worth of not less than 20 million Indian rupees according to the latest balance sheet;
- the entity should be owned and controlled by India-resident citizens or a company owned and controlled by India-resident citizens;
- the ownership of the entity should be well-diversified;
- the entity should have at least three years of experience in running the business or activity of processing information for the support or benefit of credit institutions and should have a clean track record;
- the entity, or its promoters or directors, should not have been convicted of any offence involving moral turpitude or any economic offence; and

- the entity should have a certification from a Certified Information Systems Auditor that it has a robust and secure IT system in place for preserving and protecting the data related to credit information.

Apart from the exhaustive list of specified users provided under the CIC Act and regulations made thereunder, credit information cannot be disclosed to any other person. The CIC Act also expressly prohibits specified users who receive credit information from further disclosing such information to third parties.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

No.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

The Reserve Bank of India's directions for most regulated fintech products and services (such as peer-to-peer lending platforms, prepaid payment instruments and payment aggregators) require financial service providers to be incorporated in India – that is, to establish a local presence. Notably, even foreign entities operating as online payment gateway service providers are required to open a liaison office in India before commencing operations.

However, unregulated financial services, such as crowdfunding platforms (except for equity crowdfunding), may be undertaken without a local presence. For example, Kickstarter offers its platform in India without a local presence.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

From a consumer protection perspective, advertisements must not be misleading, and sellers and marketers are prohibited from engaging in any fraudulent activities.

However, the sale and marketing of most financial products are specifically regulated as well. Notably, for investment-related products such as mutual funds or investment in securities, the following disclaimer has to be displayed in every advertisement accompanied by a voice-over reiteration: 'Investment in securities or mutual funds market are subject to market risks, read all the related documents carefully before investing.'

Read this article on Lexology

Additionally, the Advertising Standards Council of India prohibits advertisements that invite the public to invest money from containing statements that may mislead consumers in respect of the securities offered and rates of return or terms of amortisation. Where any of the foregoing elements are contingent upon any conditions or assumptions, such conditions or assumptions must be clearly indicated in the advertisement.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

Currently, distributed ledger technology is not regulated in India.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

Currently, there are no specific laws in India that regulate the use of cryptoassets.

However, India's income tax laws were recently amended to tax income earned from cryptoassets at a rate of 30 per cent. Notably, no deductions are allowed while computing such income except the cost of acquiring such cryptoassets. Additionally, a 1 per cent tax deducted at source (TDS) is also required to be charged on certain transactions involving cryptoassets. Further, non-payment of the abovementioned TDS is also subject to a penalty that may be equal to the amount of unpaid TDS.

Regarding the promotion of cryptoassets, the Advertising Standards Council of India has issued Guidelines for Advertising and Promotion of Virtual Digital Assets and Services, which require all advertisements for cryptoassets to contain mandatory disclosures and disclaimers intended to prevent opaque and misleading advertisements.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

The issuance of tokens is not regulated in India.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

While the use of artificial intelligence (AI) is not regulated, the Securities and Exchange Board of India (SEBI) has directed all registered mutual funds using applications or software based on AI or machine learning (ML) to report and make quarterly submissions to the Association of Mutual Funds in India who will, in turn, consolidate the information and submit it to the SEBI. The purpose behind this regulatory requirement is to help the SEBI understand AI and ML adoption by the Indian financial markets and formulate future policies.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

The rules for notification or consent for change in control vary based on the kind of service provided.

For instance, non-banking financial companies (NBFCs), account aggregators and NBFC peer-to-peer (P2P) lending platforms (NBFC-P2Ps) must obtain prior written permission from the Reserve Bank of India (RBI) in the case of:

- a takeover or acquisition of control;
- a change in shareholding that would result in the acquisition of 26 per cent or more of the paid-up equity capital;
- a change in management that would result in a change of more than 30 per cent of the directors; or
- any change in shareholding that would give an acquirer the right to appoint a director.

The concerned NBFC, NBFC-P2P or account aggregator, along with the acquiring party, is also required to issue a public notice of any change in its control or management at least 30 days before effecting the sale or transfer of ownership or control.

Similarly, non-bank payment systems operators (PSOs) are required to seek RBI approval prior to:

- any takeover or acquisition of control; or
- a sale or transfer of their payment system businesses to an entity not authorised by the RBI to undertake a similar activity.

Following RBI approval, the non-bank PSO and acquiring entity are also required to issue a public notice 15 days before effecting the sale or transfer of ownership or control.

Read this article on Lexology

Notably, in cases where a non-bank PSO undergoes a change in management or directors, or is selling or transferring its payment system business to an entity authorised by the RBI to undertake a similar activity, the PSO is only required to notify the RBI of this after the fact (within 15 days).

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Bribery

Bribery in India is regulated by the Prevention of Corruption Act 1988. It expressly penalises persons, including commercial organisations, for bribing or promising to bribe a public servant. Additionally, companies in India are obligated to provide a vigil mechanism and audit committee the scope of which, among other things, should include anti-bribery policies.

Money laundering

The primary legislation governing money laundering in India is the Prevention of Money Laundering Act 2002 (PMLA). The PMLA particularly imposes obligations on all banks, financial institutions (including payment systems operators) and regulated financial intermediaries as follows:

- to verify the identity of their clients using their Aadhaar or passport;
- to appoint designated directors and a principal officer to ensure overall compliance with the PMLA; and
- to maintain records of all transactions the value of which is over 1 million Indian rupees (or as prescribed by the rules under the PMLA) for a period of five years as of the date of the transaction and furnish such information to the director appointed by the central government.

Notably, in 2020, the Financial Intelligence Unit imposed a penalty of 9.6 million Indian rupees on PayPal (an online payment gateway service provider) for not complying with reporting obligations under the PMLA. This case is noteworthy because PayPal does not undertake directly regulated financial services under a licence or authorisation, but instead acts as a technology provider that collaborates with licensed or regulated institutions (namely, banks and payment system providers). PayPal has challenged this penalty before the Delhi High Court and the matter is ongoing.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

Each sectoral regulator has incorporated the provisions of the PMLA into directions for their regulated entities. Pursuant to the PMLA, the sectoral regulators have also incorporated the requirements under it into know-your-customer (KYC), anti-money laundering (AML) and combating the financing of terrorism (CFT) regulations, including the Reserve Bank of India's KYC Directions 2016, the Insurance Regulatory and Development Authority of India's Master Circular on AML-CFT, and the Securities and Exchange Board of India's Guidelines on AML Standards and CFT.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

General law

Transfer and processing of data are primarily governed by the Information Technology Act 2000 and the rules made under it, particularly the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the SPDI Rules). The SPDI Rules impose an obligation on corporates handling the sensitive personal data of an individual – such as their password, financial information and biometric information, among others – to maintain reasonable security practices and procedures such as IS/ISO/IEC 27001 or such other requirements as approved and notified by the central government.

Such data is permitted to be transferred within and outside India when necessary for lawful contracts and after obtaining consent from the data subject. However, when such a transfer takes place, the obligation to maintain reasonable security practices and procedures is also extended to the recipient of the data.

The Indian government has also published India's proposed data protection regime – the Digital Personal Data Protection Bill (DPDP Bill). Once enacted, the DPDP Bill will replace the SPDI Rules. The DPDP Bill empowers the Indian government to notify territories to which data may be transferred and prescribe the terms and conditions subject to which such data can be transferred. Thus, additional terms and conditions may be imposed by the Indian government for the transfer of data to certain countries once the DPDP Bill is enacted.

Special law (sector-specific)

Notably, in relation to payment data, the Reserve Bank of India (RBI) requires all such data to be stored only in India. Only in the case of cross-border transactions is a copy of data permitted to be stored offshore (in addition to being stored in India). While the RBI directions

do not prohibit the processing of payment system data abroad, such data is not allowed to be stored abroad and, after processing, it must be sent back to India and deleted from foreign servers.

Further, the Guidelines on Digital Lending also impose an obligation on the RBI-regulated entities who engage a lending service provider (LSP) or a DLA to provide loans to ensure that such LSP or DLA:

- only collect and store basic minimal data of the customer (namely, their name, contact details, address, etc); and
- store all data collected under such digital lending activity is only in servers located in India and in compliance with Indian laws.

The Insurance Regulatory and Development Authority of India (IRDAI) also requires all electronic maintenance of core business records to be hosted within India.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

Entities regulated by the RBI, the Securities and Exchange Board of India (SEBI) and the IRDAI are required to comply with the regulators' outsourcing frameworks, policies and guidelines, and put in place board-approved cybersecurity and cyber resilience policies to ensure that critical assets, business functions and processes are protected against compromise and are constantly monitored to detect threats. The policies must also assess vulnerabilities, and ensure quick response and recovery. Such entities are also required to report cybersecurity incidents in the manner specified by their applicable regulators.

Some of the cybersecurity regulations issued by the regulators include:

- the RBI's Master Direction – Information Technology Framework for the NBFC Sector;
- the SEBI's: Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants and Cyber Security and Cyber Resilience framework for Mutual Funds / Asset Management Companies; and
- the IRDAI's Information and Cyber Security Guidelines.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Outsourcing by financial services companies is regulated by sectoral regulators.

The Reserve Bank of India (RBI) does not permit banks, non-banking financial companies and payment system operators to outsource their core management and decision-making

functions. Similarly, the Securities and Exchange Board of India does not permit its intermediaries to outsource core business activities and compliance functions. The Insurance Regulatory and Development Authority of India also prohibits insurance intermediaries from outsourcing investment functions, fund management, and know-your-customer and anti-money laundering compliance.

While outsourcing of other activities is permitted, regulated entities continue to bear the ultimate responsibility for the acts and omissions of their outsourced service providers. They must also put in place board-approved outsourcing policies and include certain key provisions in their outsourcing agreements to ensure stringent confidentiality and security standards.

Where financial services companies outsource activities to offshore service providers, they need to also ensure that all original records are maintained in India, and the relevant offshore regulator or applicable law of the foreign jurisdiction will not prevent them from exercising appropriate control, supervision and compliance with Indian law.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

The regulatory guidelines issued by sectoral regulators on outsourcing and data protection apply to the use of cloud computing. Additionally, on 10 April 2023, the RBI notified the Master Direction on Outsourcing of Information Technology Services (IT MD), which provides that entities must adopt and demonstrate a well-established and documented cloud adoption policy. This policy should:

- identify the activities that can be moved to the cloud;
- enable and support the protection of various stakeholder interests; and
- ensure compliance with regulatory requirements on privacy, security, data sovereignty, recoverability and data storage requirements, aligned with data classification.

Such a policy must also provide for appropriate due diligence to manage and continually monitor the risks associated with cloud service providers (CSPs). The IT MD clarifies that cloud security is a shared responsibility between the outsourcing entity and the CSP.

Further, while adopting a CSP, entities must also undertake a comprehensive risk assessment of the CSP including an assessment of its cyber security capabilities.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

In India, computer code is included within the definition of a literary work and, therefore, may be protected under copyright law. Acquisition of copyright is automatic and does not require any formal procedure. However, obtaining a certificate of registration of copyright acts as prima facie evidence in disputes regarding ownership.

On the other hand, under the Patents Act 1970, a computer program is not patentable. Nevertheless, software can be patented if it is attached to an invention and if it is a component of such an invention. For an invention to be patentable, it must involve an inventive step (namely, it must be non-obvious, technically advanced or have economic significance, and must be capable of industrial application). To obtain a patent, the true and first inventor or their assignee must file an application with the Indian Controller of Patents along with the specifications of the invention.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

When a copyrightable work is made during the course of the author's employment under a contract of service, provided that there is no contract to the contrary, the employer will be the owner of the copyright. Thus, the ownership of the copyright belongs to the employer over anything produced or done by the employee in the course of employment.

As for patents, however, the inventor is regarded as the true and first owner of the patent, regardless of whether it was invented in the course of employment. The law does not provide for granting ownership rights to the employer. However, the employee may assign their invention to the employer and may be contractually obligated to do so under their employment agreement.

For IP developed by contractors or consultants, the ownership of such IP will remain with the consultant or contractor unless there is an agreement that states otherwise.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

For joint owners of patents, each co-owner's consent is required for licensing and assigning (among other things) the patent.

Similarly, in relation to copyrights, the courts in India have laid down that a joint owner of a copyright cannot, without the consent of the other joint owner, grant a licence or interest in the copyright to a third party.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

India does not have any special piece of legislation protecting trade secrets. However, they are protected through the law of contracts and other civil proceedings, such as breach of confidence. As there is no law governing its protection, when the trade secret is in itself the subject matter of the suit, for the court to be able to determine breach, the secret will have to be revealed to the court.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

In India, branding is protected under the Trade Marks Act 1999. Every 'mark' (the definition of which includes brands) that can be represented graphically and that is capable of distinguishing the goods or services of one person from another can be trademarked.

To obtain a trademark, any person claiming to be the proprietor of the mark or who proposes to use a mark can apply to the Registrar of Trademarks for registration of the mark. In the application, the applicant must also specify the class or classes of goods or services under which an application is being made.

Upon acceptance of the application, the Registrar of Trademarks will place a public advertisement to invite any opposition from individuals who may claim to be owners of the mark or a similar mark. Once opposition proceedings, if any, are completed, the Registrar of Trademarks will grant or refuse to grant the trademark. A trademark, once granted, will be valid for a period of 10 years and can then be renewed periodically.

Fintech businesses (and others) can run a class-wise trademark search on the government of India's public search of trademarks website to ensure that they do not infringe the rights of existing brands.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

If a company's or an individual's IP rights are infringed, such a person may file a civil suit for infringement before the courts. When an IP right is infringed upon, the owner of the right can apply to the courts for an injunction (restraining the person from using the IP), an account of profits, damages and the destruction of goods.

Read this article on Lexology

Notably, the Copyright Act 1957 and the Trademarks Act 1999 also provide for criminal penalties. However, intention to infringe is an important factor considered by the courts when imposing such criminal penalties.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

The Competition Commission of India regulates competition and antitrust issues in India, including anti-competitive agreements, abuse of dominance and M&A. In the recent past, CCI has investigated several M&A deals in the fintech space and has given its nod to the biggest takeover in the fintech space. CCI has also been conducting probes into a major mobile app store's payments and billing policies.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

Under the Indian income tax laws, a deduction of 100 per cent of the total income derived by an eligible start-up from an eligible business is allowable for three consecutive assessment years out of 10 years as of the date the start-up is incorporated. An eligible start-up is a company or limited liability partnership:

- that was incorporated after 1 May 2016 and before 1 May 2023;
- the total turnover of which does not exceed 1 billion Indian rupees for the year the deduction is claimed; and
- that holds a certificate of eligible business from the Inter-Ministerial Board of Certification as notified by the Indian government.

The term 'eligible business' means a business carried out by an eligible start-up engaged in innovation, development or improvement of products, processes or services, or a scalable business model with a high potential for employment generation or wealth creation.

In addition to the above, some of the following benefits may be available if the fintech company is located in an international financial services centre (IFSC):

- a deduction of 100 per cent of the gross total income earned by a unit in an IFSC is allowed for 10 consecutive years out of 15 years subject to the satisfaction of certain conditions;

- a unit located in an IFSC can opt for payment of tax at a concessional tax rate of 25.17 per cent in addition to claiming a benefit of a 100 per cent deduction of the income derived from operations in an IFSC; and
- a concessional minimum alternate (tax on book profits) tax rate of 9 per cent is applicable to a unit or company located in an IFSC that derives its income solely from convertible foreign exchange.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

Equalisation levy

A digital tax in the form of an equalisation levy (EL) is levied on payments received by a non-resident service provider. EL is charged at 2 per cent on the consideration received or receivable by an e-commerce operator without a permanent establishment in India from e-commerce supply or services made, provided or facilitated to:

- Indian residents;
- non-residents when the e-commerce supply or services made, provided or facilitated by the e-commerce operator is in the nature of:
    - sale of advertisement, which targets a customer who is resident in India or a customer who accesses the advertisement through an internet protocol address located in India; or
    - sale of data, collected from a person who is resident in India or from a person who uses an internet protocol address located in India; or
- a person (irrespective of being resident or non-resident in India) who buys such goods or services, or both, using an internet protocol address located in India.

EL shall not be applicable where:

- the e-commerce operator has a permanent establishment in India and such services are effectively connected with the permanent establishment; or
- the total consideration received by the e-commerce operator from the e-commerce supply or services made, provided or facilitated by it to persons is less than 20 million Indian rupees during the previous year.

Significant economic presence

A non-resident person is subject to tax in India in respect of income that accrues or arises in India, or is deemed to accrue or arise in India. Any income accruing or arising directly or indirectly, through or from a business connection in India, any asset or source of income in India, or transfer of capital situated in India is deemed to accrue or arise in India.

A non-resident in India is deemed to constitute a business connection in India through a significant economic presence (SEP) if:

- the non-resident carries out transactions in any goods, services or property with any Indian resident including the provision or download of data or software in India, if the value of the aggregate payments exceeds 20 million Indian rupees; or
- the non-resident engages in systematic and continuous soliciting of business, or is in interaction with a minimum of 300,000 users in India.

The income generated by a non-resident from such SEP will be taxable in India.

Note that SEP status will be constituted irrespective of whether the agreements are entered, or services are rendered, in India or outside India. The SEP-based nexus rule is not only limited to digital transactions and applies equally to cross-border transactions executed offline.

However, this is subject to the provisions of the tax treaty entered into between India and the foreign country where the non-resident with a SEP is a tax resident.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

No.

UPDATE AND TRENDS

Current developments

41 Are there any other current developments or emerging trends to note?

One of the latest fintech trends in India is apps that provide access to multiple financial and other services, all in a single app. Big Tech companies that are tailoring their products in India to incorporate these innovations are following suit. One such example is WhatsApp, a messaging platform that is now also offering Unified Payments Interface (UPI) services.

Other notable trends include:

- the rise of neo-banks, which offer all banking services efficiently, with no physical branches, using artificial intelligence;
- UPI Lite, an on-device wallet that will enable quick response code-based payments offline;
- credit cards linked to UPI;
- embedded lending; and
- the electronic version of the physical rupee (central bank digital currency) backed by blockchain technology.

Read this article on Lexology

However, maintaining a balance between the interests of fintech companies and traditional banks is proving to be tricky for the Reserve Bank of India, especially in relation to neo-banks and digital lending.

Probir Roy Chowdhury	probir@jsalaw.com
Yajas Setlur	yajas.setlur@jsalaw.com
Kumarmanglam Vijay	k.vijay@jsalaw.com
Pratish Kumar	pratish.kumar@jsalaw.com
Nikhil George	nikhil.george@jsalaw.com

Level 3 Prestige Obelisk, 3 Kasturba Road, Bengaluru 560001, India
Tel: +91 80 4350 3600
www.jsalaw.com

Read more from this firm on Lexology

Read this article on Lexology

Indonesia

Winnie Yamashita Rolindrawan, Ruth M Ginting and Farrah Azizah Habibie
SSEK Law Firm

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 266
General innovation climate 266
Government and regulatory support 267

FINANCIAL REGULATION 267
Regulatory bodies 267
Regulated activities 268
Consumer lending 269
Secondary market loan trading 269
Collective investment schemes 270
Alternative investment funds 270
Peer-to-peer and marketplace lending 270
Crowdfunding 271
Invoice trading 271
Payment services 271
Open banking 272
Robo-advice 272
Insurance products 273
Credit references 273

CROSS-BORDER REGULATION 274
Passporting 274
Requirement for a local presence 274

SALES AND MARKETING 275
Restrictions 275

CRYPTOASSETS AND TOKENS 275
Distributed ledger technology 275
Cryptoassets 276
Token issuance 276

ARTIFICIAL INTELLIGENCE 277
Artificial intelligence 277

CHANGE OF CONTROL 277
Notification and consent 277

Read this article on Lexology

FINANCIAL CRIME 278
Anti-bribery and anti-money laundering procedures 278
Guidance 278

DATA PROTECTION AND CYBERSECURITY 278
Data protection 278
Cybersecurity 279

OUTSOURCING AND CLOUD COMPUTING 279
Outsourcing 279
Cloud computing 279

INTELLECTUAL PROPERTY RIGHTS 280
IP protection for software 280
IP developed by employees and contractors 280
Joint ownership 280
Trade secrets 280
Branding 281
Remedies for infringement of IP 281

COMPETITION 281
Sector-specific issues 281

TAX 281
Incentives 281
Increased tax burden 282

IMMIGRATION 282
Sector-specific schemes 282

UPDATE AND TRENDS 283
Current developments 283

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

The use of and demand for financial technology and digital financial products in Indonesia continues to increase, with no signs of slowing. While many potential new players are considering or are in the process of entering the Indonesian market, with payment systems, digital banking, peer-to-peer lending and cryptocurrency trading areas of particular interest, we also see a growing trend of companies exploring the development of new digital finance solutions and services, including fintech software-as-a-service solutions.

The Indonesian government continues to find ways to accelerate and advance financial inclusion in Indonesia and has responded to the continued development and growth of financial technology in Indonesia by updating the regulatory framework for the sector, as the authorities seek to keep pace with fintech business players. On 12 January 2023, the Indonesian government enacted Law No. 4 of 2023 regarding the Development and Strengthening of

Read this article on Lexology

the Financial Sector (the P2SK Law), which further strengthens the government's efforts to facilitate and regulate the development of the fintech sector in Indonesia. Under the P2SK Law, Indonesia's central bank, Bank Indonesia (BI), and the Financial Services Authority (OJK) are required to coordinate in regulating, supervising, and implementing technology innovations in the financial sector, including sandbox mechanisms.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

The Indonesian government, the Indonesian central bank, the BI and the OJK are the main authorities regulating the fintech sector and have remained committed to supporting financial innovation in Indonesia with the hope of strengthening the national digital economy. To achieve this, the authorities have taken steps to provide a more accommodating regulatory framework to stimulate financial innovation. An example of this is the recently introduced sandbox provisions in the P2SK Law, which designate the OJK and the BI as the relevant authorities tasked with keeping pace with financial innovation.

In addition to its efforts to accommodate financial innovation by updating the regulatory framework, the Indonesian government regularly organises networking events for fintech players, the government, as the regulatory authority, investors, financial institutions and other stakeholders, both national and international. This includes the annual Indonesian Fintech Summit held every year since 2019, organised by the BI, the OJK and several nationwide fintech associations recognised by the Indonesian government. This summit brings together stakeholders to discuss recent developments and regulatory changes, and to strategise ways to expedite the digitalisation of the financial services industry and push economic growth.

The Indonesian government is also attempting to balance support for fintech development and innovation with the protection of Indonesian consumers and the public, as evidenced by the recent issuance of the P2SK Law.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

Fintech products and services in Indonesia are regulated mainly by two government bodies, the BI and the Financial Services Authority (OJK). The BI's authority is primarily geared toward payment system operators, while the OJK oversees bank and non-bank financial institutions. In the case of certain entities such as banks, both the OJK and the BI have jurisdiction, over regulating their products and services. Specifically, fintech products relevant to payment systems come under the oversight of the BI.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

In general, all parties that conduct business activities in Indonesia are subject to licensing and registration requirements under the authority of the Ministry of Investment and the Indonesian Investment Coordinating Board. For businesses in the financial sector, there are additional specific licensing requirements under the authority of the BI or the OJK.

For business activities that fall under the authority of the BI, such as payment systems, whether licensing requirements are triggered depends on the scope of business activities in which a company engages. For example, business actors in the payment system sector engaged only in pre-transaction or post-transaction steps (namely, activities outside the authorisation, clearing and final settlement stages) will be deemed as supporting providers, which would not trigger any licensing requirement from the BI. The same applies to business activities that fall under the authority of the OJK and whether they will trigger a licensing requirement.

Innovations within the fintech sector in Indonesia are subject to licensing requirements. Prior to the enactment of Law No. 4 of 2023 regarding the Development and Strengthening of the Financial Sector (the P2SK Law), these were solely regulated under OJK Regulation No. 13/POJK.02/2018, dated 16 August 2018, concerning Digital Financial Innovation in the Financial Services Sector (OJK Regulation 13). Activities considered as digital financial innovation under OJK Regulation 13 include transaction settlement, capital raising via equity crowdfunding and smart contracts, advanced algorithm-driven investment management, fundraising and fund disbursement activities like peer-to-peer lending, insurance provisions facilitated by the sharing economy and digital distribution, market support via artificial intelligence and big data, digital finance activities such as Islamic digital financing and robo-advisers, and other financial services like invoice trading and blockchain-based applications.

The P2SK Law broadens the scope of technology innovation and introduces the concept of the Technology Innovation in the Financial Sector (ITSK) cluster. In contrast to digital financial innovations, which were solely under the OJK's supervision, the ITSK falls under the jurisdiction of both the OJK and the BI, whose supervision shall depend on the specific activities. This spectrum of activities includes payment systems, securities transaction settlement, capital raising, investment management, risk management, fund collection and (or) disbursement, market support, activities involving digital financial assets including cryptocurrencies, and other digital financial services.

Foreign organisers of trade through an electronic system (PPMSEs), which is any business practitioner that provides electronic communication facilities used in trade transactions and operates from outside Indonesia and fulfils certain criteria, shall be required to appoint a representative in Indonesia and consequently must have a foreign trade company representative office in the country.

Consumer lending

5 Is consumer lending regulated in your jurisdiction?

Consumer lending is regulated in Indonesia, with a particular focus on IT-based money lending services (peer-to-peer lending), as regulated under OJK Regulation No. 10/POJK.05/2022 regarding Information Technology-Based Co-Financing Services, dated 29 June 2022 (OJK Regulation 10/2022). This regulation requires providers of IT-based co-financing services to be a limited liability company and meet certain prerequisites.

The OJK has the authority to regulate, register and issue licences, as well as supervise the fintech consumer lending industry. Pursuant to this regulation, a company engaging in the provision of peer-to-peer lending activities can have a maximum foreign ownership of 85 per cent, which means at least 15 per cent of the ownership must be in the hands of Indonesian parties.

Further, the provider must have at least 25 billion rupiahs (approximately US$1.7 million at current exchange rates) in issued capital during its establishment. The issued capital must be fully paid and placed in a time deposit (*deposit berjangka*). Providers must also have a minimum equity of 12.5 billion rupiahs (approximately US$850,000 at current exchange rates) at all times. The fulfilment of this minimum equity requirement can be done gradually, as follows:

- at least 2.5 billion rupiahs for one year as of the promulgation of OJK Regulation 10/2022;
- at least 7.5 billion rupiahs for two years as of the promulgation of OJK Regulation 10/2022; and
- at least 12.5 billion rupiahs beginning three years from the promulgation of OJK Regulation 10/2022.

Peer-to-peer providers shall directly apply to the OJK for a licence. The OJK further requires providers to obtain an Electronic System Provider Certificate (ESP Registration Certificate) issued by the Ministry of Communication and Informatics, in addition to the licence issued by the OJK. Providers are restricted from conducting any funding activity before obtaining an ESP Registration Certificate. Within 30 calendar days after obtaining a TDPSE, providers must begin funding activity. Failure to obtain a TDPSE or to conduct funding within the given timeline will result in the OJK cancelling the provider's existing licence.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

Currently, the trading of loans in the secondary market in Indonesia is not specifically regulated and there is no specific restriction on this activity.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Under Indonesian law, two types of collective investment schemes are recognised: Collective Investment Contracts (CIC) and Joint Investment Contracts (JIC). A CIC is a contract in which an investment manager and a custodian bank jointly bind investors. In this arrangement, the investment manager is authorised to manage the collective investment portfolio, while the custodian bank is responsible for implementing collective custody. This is often structured as a mutual fund.

A JIC is managed by a venture capital company with the approval of the OJK, even though a JIC is not considered a legal entity in Indonesia. However, entities established through venture fund JICs are deemed as legal entities.

It is important to note that alternative finance products or services, such as peer-to-peer lending, do not fall within the purview of these regulations. They are instead subject to their own specific regulations.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

In general, investment managers are regulated by the OJK, pursuant to OJK Regulation No. 24/POJK.04/2014 regarding Implementation Guidelines for the Functions of Investment Managers, dated 19 November 2014. The roles of investment managers are also regulated under the following regulations:

- OJK Regulation No. 34/POJK.05/2015 regarding Business Licensing and Institutional Matters of Venture Capital Companies, dated 28 December 2015 (OJK Regulation 34/2015); and
- OJK Regulation No. 23/POJK.04/2016 regarding Mutual Funds in the Form of Investment Collective Contracts, dated 19 June 2016, as amended by OJK Regulation No. 4/POJK.04/2023, dated 31 March 2023 (OJK Regulation 23/2016).

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

While marketplace lending is not specifically regulated in Indonesia, peer-to-peer lending is. The activity of peer-to-peer lending is specifically regulated under OJK Regulation No. 10/POJK.05/2022 regarding Information Technology-Based Co-Financing Services, dated 4 July 2022. It provides the OJK with the right to regulate and supervise peer-to-peer lending activities, including handling the registration and licensing of peer-to-peer lending platform providers. Peer-to-peer lending in Indonesia is described as the provision of financial

services, whereby the lender meets the borrower in conducting conventional funding or based on *shariah* principles directly through an electronic system using the internet.

Shareholders in peer-to-peer lending companies can be Indonesian individuals or legal entities or a combination of Indonesian and foreign individuals or legal entities. The funding limit is set at 2 billion rupiahs (approximately US$135,000 at current exchange rates) for both the funding receiver and provider. Members of the board and officials must have competency certification issued by a professional certification institution in the financial technology sector. Foreign board members must obtain Bahasa Indonesia certification within one year of approval. Primary parties, including controlling shareholders, board members and commissioners, must pass a fit-and-proper test before taking any actions. Additional requirements for peer-to-peer Providers include electronic system requirements, risk management and internal audit obligations, and controlling shareholder requirements.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

Equity crowdfunding covers the provision of share-offering services conducted by issuers to sell shares directly to investors through an open electronic system network. Equity crowdfunding is regulated under OJK Regulation No. 57/POJK.04/2020 regarding Securities Offerings Through Information Technology-Based Crowdfunding Services, dated 11 December 2020, as amended by OJK Regulation No. 16/POJK.04/2021, dated 26 August 2021. Under this regulation, a licensed equity crowdfunding platform provider or organiser is able to provide issuers (Indonesian limited liability companies) access to sell their shares to investors that are also using the platform. An equity crowdfunding platform company is required to be an Indonesian limited liability company or an Indonesian cooperative and have registered with and received a licence from the OJK to provide, manage and operate the equity crowdfunding platform.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

The prevailing regulations do not specifically address invoice trading in Indonesia.

Payment services

12 | Are payment services regulated in your jurisdiction?

Payment services in Indonesia are regulated mainly by Indonesia's central bank, the BI, which is in charge of regulating payment system activities in Indonesia. Following the issuance of BI Regulation No. 22/23/PBI/2020 regarding Payment Systems (BI Regulation 22/23), dated 30 December 2020, the BI issued several additional regulations that contain more specific and robust provisions with respect to payment system providers (PSPs) and payment system infrastructure providers (PSIPs). These additional regulations are BI Regulation No. 23/6/PBI/2021 regarding Payment System Providers, dated 1 July 2021 (BI Regulation 23/6), and BI Regulation No. 23/7/PBI/2021 regarding Payment System Infrastructure Providers, dated 1 July 2021 (BI Regulation 23/7). PSPs are open to 85 per cent foreign share ownership (with

a maximum of 49 per cent of shares with voting rights held by foreign shareholders), while PSIPs are open to 20 per cent foreign share ownership (with a 20 per cent maximum of shares with voting rights held by foreign shareholders).

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

In response to the evolving open banking activities within the payment system sector, the BI enacted Members of the BI Board of Governors Regulation No. 23/15/PADG/2021, which parties were required to comply with by 31 December 2022 at the latest. This regulation introduced the National Standard for Open Application Programming Interface (API) Payment, also known as the SNAP policy. The SNAP policy outlines a standardised approach to Open API Payment, aiming to ensure its effective and efficient operation.

One of the key objectives of the SNAP policy is to provide clarity regarding its scope and application, as well as to delineate the roles and responsibilities of various parties involved in the administration of Open API Payment connectivity.

The SNAP policy also aims to ensure a level playing field among different payment service providers, including both banks and non-bank institutions, as well as other parties that collaborate in Open API Payment connectivity. This is aligned with broader efforts to foster a cohesive and integrated Open API Payment ecosystem.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Robo-advisory services are mentioned in both OJK Regulation 13 and the P2SK Law as part of digital financial innovation and technological innovation in the financial sector that is considered other digital finance supporting activities. Thus, the use of robo-advisory services in financial products is allowed, subject to the limitations provided in OJK Regulation 13 and the P2SK Law, as well as any regulation specific to the financial product being offered.

Further, the Commodity Futures Trading Supervisory Body (Bappebti), under the Ministry of Trade, has issued Bappebti Regulation No. 12 of 2022 regarding the Organization of the Submission of Information Technology-Based Advice in the Form of an Expert Advisor in the Field of Commodity Futures Trading, dated 2 September 2022 (Bappebti Regulation 12/2022), which regulates IT-based advice in the form of an expert adviser. IT-based advice is defined as an IT-based tool that is structured based on algorithms that are implanted in the lines of its computer program, which are determined based on the characteristics, types, needs, and expectations of a client. This IT-based advice is capable of working automatically to conduct market monitoring, calculation of market entry or exit opportunities, placing reasonable transactions, and risk management by taking into account the needs of each client. IT-based advice may only be provided by futures advisers who have obtained

approval from Bappebti and may only be in the form of information and (or) recommendations regarding the sale and purchase of commodities based on futures contracts, *shariah* derivative contracts, and (or) other derivative contracts.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

The selling and marketing of insurance products in Indonesia by both insurance companies and fintech companies is regulated and licensed by the OJK. In practice, licensed insurance companies in Indonesia have been selling their products over the internet, through their own platforms or by cooperating with other parties (eg, e-commerce platforms or e-money platforms) to assist in facilitating the selling and marketing of their insurance products. However, it is important to note that fintech companies involved in the selling or marketing of insurance products face certain limitations, as specific rights are exclusively reserved for insurance companies.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

There are restrictions on providing credit information services. In Indonesia, credit reports can only be issued by a credit bureau licensed by the OJK. A credit report is defined under OJK Regulation 5/POJK.03/2022 regarding Credit Information Management Agencies, dated 28 March 2022, and OJK Circular Letter No. 27/SEOJK.03/2022 of 2022 regarding Credit Information Management Agencies, dated December 22, 2022 (together, the Credit Bureau Regulation), as a product or service generated by a credit bureau in writing, verbally or by some other method, sourced from credit data and other data owned by the credit bureau. A credit report generated by a credit bureau, among other things, contains information on:

- statistics for planning, business development and determining policies;
- information to measure the performance and supervise the risk profile of the debtor or customer;
- the ability of the debtor or customer to fulfil its fund provision obligations;
- the character of the debtor or customer; and
- other information that may be utilised to assess the abilities of the debtor or customer.

Pursuant to the Credit Bureau Regulation, a credit bureau engages in the business activities of collecting credit data and other data, and processing credit data and other data to generate credit information.

The Credit Bureau Regulation also specifically mentions that a credit bureau must be in the form of an Indonesian limited liability company and is subject to applicable foreign shareholding restrictions. In addition, a credit bureau must obtain a business licence from the OJK to conduct its business activities. While the total ownership of one or more foreign parties in a credit bureau is limited to 20 per cent, if one foreign party owns more than

one credit bureau that foreign party's total ownership in all the credit bureaus combined is limited to 20 per cent.

In collecting and processing credit information, a licensed Indonesian credit bureau obtains credit data from the OJK. The credit data from the OJK consists of data submitted to it by financial institutions. A licensed Indonesian credit bureau may also cooperate with financial institutions to obtain credit data or with financial institutions and non-financial institutions for other data or both. A credit bureau must make an effort to ensure that the source of the data informs the relevant debtor or customer of how the credit data and other data will be utilised. Credit data is defined as data regarding the condition of the funding facility of the debtor or the customer.

Other data in relation to a credit bureau is defined as data other than credit data that can be used to describe the capability of a certain party in fulfilling the party's financial obligations including the behavioural patterns of the debtor or customer.

In addition to traditional credit bureau scores, Indonesian law also regulates alternative credit scoring mechanisms, which fall under the scope of digital technology innovation under the supervision of the OJK. However, there are restrictions on the type of data that can be used to generate such credit scores. Obtaining a licence from the OJK is a prerequisite to operate in this cluster.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

The prevailing laws and regulations in Indonesia do not recognise the concept of passporting, and regulated activities cannot be passported into Indonesia.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

In general, to obtain a licence from the Indonesian government to provide financial services in Indonesia, a party must establish a local presence.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

All activities with respect to the sale and marketing of financial services and products in Indonesia must be conducted by licensed entities. Further, generally, the people providing financial services to the public must meet certain competency standards, as evidenced by the obtainment of certification from a registered certification institution approved by the Financial Services Authority. The sectors that require competency certification include capital markets and banking.

Additionally, there are regulations for the sale and marketing of financial services and products in the traditional sense, such as conventional banking, investment and insurance. There is far less clarity regarding the organisation of the sale and marketing of unconventional financial services, for example, investments related to cryptocurrency and initial coin offerings. The main principle of sales and marketing by financial and fintech businesses is a prohibition on misleading information and causing a loss for consumers.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

While there is no specific rule or regulation for blockchain or distributed ledger technology in Indonesia, it is referred to in regulations issued by the BI, the Financial Services Authority (OJK) and the Commodity Futures Trading Supervisory Body (Bappebti), which aim to support innovative industry players in the financial services and payment systems fields.

Blockchain technology is mentioned in BI Regulation 23/6, which provides that the use of blockchain technology or distributed ledger technology for fund transfers, electronic money, electronic wallets or mobile payments is considered as providing financial technology in the payment system sector. It is also mentioned in OJK Regulation 13 as an example of digital financial innovation related to other financial services activities, such as invoice trading, vouchers and tokens. Further, Bappebti Regulation No. 8 of 2021 regarding Guidelines for Organising Crypto Asset Physical Trading Market on the Futures Exchange, as amended by Bappebti Regulation No. 13 of 2022, dated 9 November 2022 (together, Bappebti Regulation 8/2021), also mentions distributed ledgers in its description of cryptoassets.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

The crypto industry in Indonesia falls under the auspices of Bappebti, under the Ministry of Trade (MOT) and in coordination with other institutions such as the OJK, the BI and the Ministry of Communication and Informatics. The MOT has acknowledged cryptoassets, including but not limited to digital coins (virtual currency or cryptocurrency), as tradable commodities for which Bappebti acts as the regulator and supervisor. Nevertheless, through the enactment of Law No. 4 of 2023 regarding the Development and Strengthening of the Financial Sector (the P2SK Law), the authority over cryptoassets shall be transferred from Bappebti to the OJK.

As regulated under Bappebti Regulation No. 8 of 2021 regarding Guidelines for Organising Crypto Asset Physical Trading Market on the Futures Exchange, as amended by Bappebti Regulation No. 13 of 2022, dated 9 November 2022 (together, Bappebti Regulation 8/2021), the trade of cryptoassets shall be facilitated by crypto asset physical traders (crypto exchanges).

Bappebti Regulation 8/2021 defines cryptoassets as intangible commodities in digital form, using cryptography, IT networks and distributed ledgers to regulate the creation of new units, verify transactions and secure transactions without the intervention of other parties. In essence, cryptoassets may be traded if they have been approved by the head of Bappebti.

Applicable laws and regulations do not explicitly distinguish between security tokens, utility tokens, stablecoins and deposit coins, and the forgoing assets are generally treated the same as cryptoassets. The Indonesian government is also yet to issue a specific regulation regarding NFTs.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Currently, there are no specific laws or regulations surrounding STOs, ICOs and other token generation events. It is noteworthy that Bappebti has explicitly clarified that the current regulations concerning cryptocurrency do not encompass ICOs or initial token offerings.

According to Bappebti Regulation No. 11 of 2022 regarding the Determination of the List of Tradable Crypto Assets within the Crypto Asset Physical Market, as of August 8, 2022, cryptoassets (including tokens) can only be traded if they are listed in Bappebti Regulation 11/2022. Crypto exchanges wishing to list a cryptoasset can submit a proposal for its inclusion through the Crypto Asset Futures Exchange or Futures Exchange. The Futures Exchange and the Crypto Asset Committee will then assess the proposal before submitting a recommendation to Bappebti.

Read this article on Lexology

If, however, the Futures Exchange and the Crypto Asset Committee have not yet been established (which is currently the case), the proposal's assessment and evaluation can be handled by the Crypto Asset List Assessment Team. This team is composed of representatives of Bappebti, crypto asset trading associations and registered business actors in the cryptoasset physical market.

In practice, it is not unusual for licensed crypto exchanges to trade cryptoassets that are not listed in Bappebti Regulation 11/2022, even though doing so may expose them to potential administrative sanctions from Bappebti.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

Presently, there is no specific law or regulation that addresses the use of artificial intelligence (AI), including robo-advice. However, AI and robo-advice are mentioned in Financial Services Authority (OJK) Regulation 13 and Law No. 4 of 2023 regarding the Development and Strengthening of the Financial Sector (the P2SK Law) as part of digital financial innovation and technological innovation in the financial sector that is considered a market support activity and other digital finance supporting activities. This includes machine-readable news, social sentiment, big data, market information platforms and automated data collection and analysis. Thus, the use of artificial intelligence in financial products is allowed, subject to the limitations provided in OJK Regulation 13 and the P2SK Law, as well as any regulation specific to the financial product being offered.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

The rules relating to notification or consent requirements in a change of control depend on the business activities and the specific licence held by the entity. As a matter of general principle, entities holding a licence in the financial services sector and the payment system services sector typically need to obtain prior approval from the central bank, the BI or the Financial Services Authority (OJK) if a change of control occurs. There are certain sectors that only require the submission of a notification and not approval. Additionally, change of control in all financial sectors shall also be notified to the Ministry of Law and Human Rights.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

In general, fintech companies are required to implement anti-money laundering (AML) procedures and need to conform to anti-bribery regulations in Indonesia. For example, players in the cryptocurrency sector in Indonesia, including cryptocurrency traders and futures exchanges, are required to have in place AML procedures and prevention of terrorism funding and proliferation of mass destruction weapons guidelines, pursuant to Commodity Futures Trading Supervisory Body (Bappebti) Regulation No. 8 of 2021 regarding Guidelines for Organizing Crypto Asset Physical Trading Market on the Futures Exchange, dated 29 October 2021, as amended by Bappebti Regulation No. 13 of 2022 dated 9 November 2022 (Bappebti Regulation 8/2021).

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

Currently, there is no extensive regulatory or industry-wide anti-financial crime guidance aimed specifically at fintech companies. However, both the BI and the Financial Services Authority (OJK) have issued certain regulations applicable to financial sectors, including the financial service sector and payment system sector. These regulations cover the prevention of money laundering and terrorism financing. For the OJK, these issues are governed by OJK Regulation No. 12/POJK.01/2017, issued on 21 March 2017, and subsequently amended by OJK Regulation No. 23/POJK.01/2019, dated 30 September 2019. For the BI, they are regulated under BI Regulation Number 19/10/PBI/2017, which pertains to the Implementation of Anti-Money Laundering and Terrorism Financing Prevention for Non-Bank Payment System Service Providers and Non-Bank Foreign Exchange Business Activities, dated 11 September 2017.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The main laws and regulations relevant to personal data protection and transfers are:

- Law No. 27 of 2022 regarding Data Protection (Indonesian PDP Law);
- Law No. 11 of 2008 regarding Electronic Information and Transactions, dated 21 April 2008, as amended by Law No. 19 of 2016, dated 25 November 2016;
- Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions, dated 10 October 2019; and

- Ministry of Communication and Informatics Regulation No. 20 of 2016 regarding Personal Data Protection in Electronic Systems, dated 1 December 2016.

The Indonesian PDP Law permits domestic data transfers while imposing specific requirements for cross-border data transfers. Specifically, the receiving country must have a level of data protection that is either equivalent to or greater than that of Indonesia. If these conditions are not met, the data subject must provide explicit consent for the cross-border data transfer.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

There are, to date, no specific cybersecurity regulations or standards applicable across the fintech sector in Indonesia. Different sectors may also have different cybersecurity requirements and standards for their respective business activities. However, the National Cyber and Encryption Agency (BSSN) has set out general regulations or standards for information security management, which includes cybersecurity under BSSN Regulation No. 8 of 2020 on Security Systems in the Operation of Electronic Systems, dated 14 July 2020. Fintech companies may be subject to the provisions of this regulation if they use an electronic system in the operation of their business. Under this regulation, certain security standards must be implemented by the electronic system operator, including SNI ISO/IEC 27001 and other cybersecurity standards required by the BSSN or other ministries or institutions.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

There is no specific legal requirement or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business. However, different sectors may have different outsourcing requirements and standards for their respective business activities.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

There are no specific legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry. However, cloud computing is generally regulated under Ministry of Communication and Informatics (MOCI) Regulation No. 5 of 2020 regarding Electronic System Providers in the Private Sector, dated 24 November 2020, as amended by MOCI Regulation No. 10 of 2021, dated 21 May 2021.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Under Indonesian laws and regulations on intellectual property rights, a computer program, which, consequently, includes software, is regulated under Law No. 28 of 2014 regarding Copyrights, dated 16 October 2014. Copyright protection for computer programs is automatically provided by this law, without requiring the registration of the computer program.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

In principle, the IP rights will remain with the creators, which in this instance is the employee or contractor or consultant, unless stated otherwise in an agreement. To avoid any uncertainty, it is common practice in Indonesia for employers to include a clause in employment agreements with employees or contractors or consultants that clearly states that the IP rights of any creation will be solely owned by the employer.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

There is no such restriction under Indonesian law.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Law No. 30 of 2000, issued on 20 December 2000 (the Trade Secret Law), provides a very generic approach to the definition of a trade secret. A trade secret is defined as information that is not publicly known in the fields of technology or business, with an economic value owing to its usefulness in a business activity, and whose confidentiality is kept by the owner of the trade secret. The Trade Secret Law indicates that trade secrets are inherently protected without needing to undergo a specific procedure. Holders of trade secrets may bring a claim for compensation and a cease-and-desist action. Court proceedings involving trade secrets may be held confidentially upon the request of a party in the case.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Under Law No. 20 of 2016 regarding Marks and Geographical Indications, dated 25 November 2016, as amended by Government Regulation in Lieu of Law No. 2 of 2022, dated 30 December 2022, a brand (mark) is protected once it is registered with the relevant government IP office in Indonesia. As a precautionary action, a fintech business can check with the government IP office to see if there are similar brands or trademarks already registered in Indonesia. It can also conduct market monitoring of known brands in its industry in Indonesia.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

Individuals or companies whose intellectual property rights have been infringed may bring claims to the counterparty for compensation and a cease-and-desist action. These claims can go through commercial court, arbitration, or alternative dispute settlement.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

To date, the prevailing regulations do not address competition issues particular to fintech companies. We have not identified any specific competition issues in the fintech industry.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

There are tax incentives available for certain fintech companies under Law No. 4 of 2023 regarding the Development and Strengthening of the Financial Sector (the P2SK Law), which is part of the government's efforts to develop and strengthen the financial sector. The government may provide tax incentives for specific financial services and programmes in accordance with tax regulations. Additionally, companies conducting business in a pioneer industry may receive tax facilities, such as a reduction in corporate income tax.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

The Indonesian Minister of Finance (MOF) recently issued a regulation on income tax and value added tax (VAT) specifically for fintech businesses, namely, MOF Regulation No. 69/PMK.03/2022 regarding Income Tax and Value Added Tax for the Implementation of Financial Technology, dated 1 May 2022. For example, the income generated from a peer-to-peer lending business shall be subject to VAT and income tax. However, VAT collection is exempted for certain fund transfer transactions. The VAT rate for sectors subject to VAT collection is generally 11 per cent.

The MOF also issued a regulation to impose income tax and VAT on cryptocurrency trade transactions, namely, MOF Regulation No. 68/PMK.03/2022 regarding Value Added Tax and Income Tax on Crypto Asset Trade Transactions, dated 1 May 2022. VAT in the amount of 0.1 per cent will be imposed if the crypto trader is registered as a trader through electronic systems provider (PPMSE), or 0.2 per cent if the PPMSE is not yet registered.

To qualify as a PPMSE VAT collector, a party must have a transaction value with Indonesian purchasers that exceeds a certain threshold within 12 months, a traffic volume or a number of persons who accessed the party's platform that exceeds a certain threshold within 12 months, or both. These thresholds will be further set out by the Directorate of General Taxation. Indonesian government officials have been quoted in various media reports saying that they are targeting providers such as Netflix and Spotify that operate outside of Indonesia with a significant number of users in the country.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

There is no specific immigration scheme for fintech businesses, so the general immigration scheme is applicable. An Indonesian entity must act as the sponsor for any foreign national who will work in Indonesia, and foreign workers can only fill positions that are allowed for foreigners, as set out by the Ministry of Manpower.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

The enactment of Law No. 4 of 2023 regarding the Development and Strengthening of the Financial Sector (the P2SK Law) signifies a forthcoming shift in regulatory authority over several fintech-related sectors to either the Financial Services Authority or the Indonesian Central Bank (BI), with this shift expected to occur within the next two years. Further details regarding this transition will be addressed in a future government regulation that is currently pending.

The Indonesian government has additionally launched the central bank digital currency rupiah (digital rupiah), via the P2SK Law. The digital rupiah is officially accepted as a form of currency in Indonesia, on par with physical banknotes and coins. Despite the presently limited regulations concerning the digital rupiah, the BI's vision for its implementation is detailed in the Project Garuda White Book. This document offers a roadmap for the utilisation of digital rupiah in Indonesia, outlining the progressive stages of its application.

The issuance of the P2SK Law suggests that Indonesia is embracing technological progress while maintaining a prudent approach toward the integration of technology into the nation's routine operations and activities.

ssek LAW FIRM

Winnie Yamashita Rolindrawan winnierolindrawan@ssek.com
Ruth M Ginting ruthginting@ssek.com
Farrah Azizah Habibie FarrahHabibie@ssek.com

14th Floor Mayapada Tower I, Jl Jend. Sudirman
Kav 28, Jakarta 12920, Indonesia
Tel: +62 21 521 2038
www.ssek.com

Read more from this firm on Lexology

Read this article on Lexology

Ireland

Ian O'Mara and Joe Beashel
Matheson LLP

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 285
General innovation climate 285
Government and regulatory support 286

FINANCIAL REGULATION 287
Regulatory bodies 287
Regulated activities 287
Consumer lending 287
Secondary market loan trading 288
Collective investment schemes 289
Alternative investment funds 289
Peer-to-peer and marketplace lending 290
Crowdfunding 290
Invoice trading 290
Payment services 291
Open banking 291
Robo-advice 291
Insurance products 291
Credit references 292

CROSS-BORDER REGULATION 292
Passporting 292
Requirement for a local presence 293

SALES AND MARKETING 293
Restrictions 293

CRYPTOASSETS AND TOKENS 293
Distributed ledger technology 293
Cryptoassets 294
Token issuance 294

ARTIFICIAL INTELLIGENCE 295
Artificial intelligence 295

CHANGE OF CONTROL 295
Notification and consent 295

Read this article on Lexology

FINANCIAL CRIME	**295**
Anti-bribery and anti-money laundering procedures	295
Guidance	296
DATA PROTECTION AND CYBERSECURITY	**297**
Data protection	297
Cybersecurity	297
OUTSOURCING AND CLOUD COMPUTING	**297**
Outsourcing	297
Cloud computing	298
INTELLECTUAL PROPERTY RIGHTS	**298**
IP protection for software	298
IP developed by employees and contractors	298
Joint ownership	299
Trade secrets	299
Branding	300
Remedies for infringement of IP	300
COMPETITION	**300**
Sector-specific issues	300
TAX	**301**
Incentives	301
Increased tax burden	301
IMMIGRATION	**302**
Sector-specific schemes	302
UPDATE AND TRENDS	**302**
Current developments	302

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Ireland has a very active fintech scene and is one of the leading jurisdictions for fintech start-ups and corporate innovation in Europe. In addition, as a result of Brexit, many payments and e-money firms that previously provided services across the European Union via a UK payments or e-money licence have sought to obtain authorisation from the Central Bank of Ireland (the Central Bank) to ensure continuity of operations. This has led to a very significant increase in the number of licensed payments and e-money firms operating in the jurisdiction. As of June 2023, there were over 40 such firms formally authorised and operating in Ireland.

Ireland has won an outsized share of European investment in corporate innovation labs, with many global financial services groups establishing their innovation labs in Ireland. Accelerator programmes are also expanding their activities in Ireland, with Dublin being

added as one of two accelerator locations by the NadiFin fintech accelerator programme and the National Digital Research Centre expanding its activities outside Dublin to Waterford and Galway. Dublin remains the hub for fintech activities in Ireland, but other regional centres are also seeing growth.

Notwithstanding the burgeoning start-up scene, digital challenger banks have not penetrated the Irish market to any significant extent and there are currently no home-grown challenger banks. EU digital operators have passported their services into Ireland but have not yet posed an existential threat to traditional Irish banking houses. Robo-advice has yet to make an appearance in the mainstream investments market. Many life and health insurers are now investigating the potential incorporation of wearable devices into insurance underwriting, and some of the main motor insurers have launched safe driving apps that provide telematics-based discounts for drivers.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

The government of Ireland is strongly supportive of fintech and in its recently-revised Strategy for the International Financial Services Sector (Ireland for Finance 2025) has stated its commitment to developing Ireland as a global leader in the financial services sector, creating an environment in which both indigenous and multinational firms can draw on key governmental incentives and support to grow their businesses. The main state business and employment promotion agencies, IDA Ireland and Enterprise Ireland, provide a range of supports for fintech operations at all levels of development and the state Ireland State Investment Fund (ISIF) has made multiple venture capital and equity investments in promising fintech start-ups.

Since 2018, the Central Bank has provided the Innovation Hub for fintech companies operating in Ireland. This is a direct and dedicated point of contact for firms developing or implementing innovations in financial services based on new technologies. This intends to accommodate greater interaction by the Central Bank with the growing number of fintech businesses looking to set up operations in Dublin, or expand their existing operations both in the regulated and unregulated space. A number of initiatives have been undertaken by different financial institutions applying distributed ledger technology, artificial intelligence (AI) and robotics, and the Central Bank is keen to engage with innovators who are operating as regulated and unregulated entities in the financial services space. According to the Innovation Hub: 2021 Update, the Innovation Hub received 84 enquiries, representing a 19 per cent increase in enquiry numbers over 2020.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

The Central Bank of Ireland (the Central Bank) is the only financial services regulator in Ireland and is responsible for authorising and supervising all providers of regulated financial services. The Central Bank is responsible for both prudential supervision and conduct of business supervision of regulated entities that it has authorised. Where a regulated firm has been authorised by a supervisory authority in another EU or EEA jurisdiction, the home state regulator will be responsible for prudential supervision but the Central Bank will be responsible for the conduct of business supervision in Ireland. The Single Supervisory Mechanism at the European Central Bank also directly supervises significant credit institutions and has exclusive competence for the authorisation of credit institutions (other than branches of third-country credit institutions).

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Whether or not a fintech business is required to hold a financial services authorisation will depend on the nature of the activities that the firm engages in. As far as investment-related activities are concerned, Directive 2014/65/EU (Markets in Financial Instruments Directive II) (MiFID 2), was transposed into Irish law by the European Union (Markets in Financial Instruments) Regulations 2017 (the Irish MiFID 2 Regulations). Engaging in any of the investment services and activities listed in MiFID 2 (eg, providing investment advice or executing client orders) is a regulated activity requiring authorisation. Other parts of the MiFID 2 package also have direct effect in Ireland.

Engaging in 'banking business' requires authorisation under the Central Bank Act 1971 (the 1971 Act). The European Union (Capital Requirements) Regulations 2014 transposed the Directive 2013/36/EU (Capital Requirements Directive IV) (CRD4) into Irish law and the requirements for obtaining an Irish banking licence are based on the transposition of the CRD4 package. Other parts of the CRD4 package also have a direct effect in Ireland. 'Banking business' means taking deposits or other repayable funds from members of the public and granting credit for own account. There is a restriction in the 1971 Act, in the absence of an exemption from the Central Bank, which prohibits anyone from using the term 'bank' in their name or holding themselves out as a bank without holding the necessary authorisation. Ireland also has a regime for authorising branches of credit institutions established in third countries (third-country branches) under section 9A of the 1971 Act.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Subject to very limited exceptions, providing deferred payments, cash loans or other similar financial accommodation to individuals (not just consumers) in Ireland is a regulated activity requiring authorisation as a retail credit firm under the Central Bank Act 1997, unless the

lender is otherwise authorised to provide such credit, for example, a bank. This is an Irish domestic licensing regime and does not derive from an EU law obligation.

The legislation was further amended in early 2022 by the introduction of the Consumer Protection (Regulation of Retail Credit and Credit Servicing Firms) Act 2022. This legislation, once commenced, will bring providers of indirect credit to consumers, for example, providers of buy now, pay later agreements into the regulatory perimeter for the first time. Previously, indirect providers of consumer credit products were technically outside the scope of Irish financial services law from a licensing perspective. Since the legislation was commenced, a number of firms active in this sector have now sought transitional authorisations from the Central Bank to carry on their newly regulated credit-providing activities while they progress their authorisation applications.

Multiple aspects of consumer lending are also regulated (at the conduct-of-business level) under the Consumer Credit Act 1995 (the 1995 Act) and the European Communities (Consumer Credit Agreement) Regulations 2010 (the 2010 Regulations), which regulate the form and content of credit agreements. The 1995 Act and the 2010 Regulations implement the provisions of Directive 87/102/EEC (Consumer Credit Directive) as amended, and CRD4.

The Central Bank's Consumer Protection Code 2012 (the CPC) and associated addenda are also relevant. The CPC applies to all financial services providers who are authorised, registered or licensed by the Central Bank, as well as financial services providers authorised, registered or licensed in another EU or EEA member state when providing services in Ireland, on a branch or cross-border basis. The CPC essentially requires regulated entities to adhere to a set of general requirements, such as to provide terms of business to consumers, conduct know-your-customer, to establish the suitability of the product, and adhere to lending and advertisement requirements. The CPC is currently being reviewed by the Central Bank through a public consultation and is likely to be comprehensively overhauled in 2024.

There are also separate requirements for mortgage lending to consumers, including the 'housing loan' requirements under the 1995 Act, the European Union (Consumer Mortgage Credit Agreements) Regulations 2016, implementing the provisions of Directive 2014/17/EU (Mortgage Credit Directive) and the Central Bank's Code of Conduct on Mortgage Arrears.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

Part V of the Central Bank Act 1997 regulates credit servicing, which includes holding the legal title to loans made by regulated financial services providers to individuals and small and medium-sized (SME) businesses. Credit servicing is a regulated activity requiring authorisation by the Central Bank. Acquiring the beneficial interest in such loans is not a regulated activity, however, although there are associated licensing requirements applicable to entities that provide administration or servicing in respect of such loans. Trading non-SME corporate loans is not, generally speaking, a regulated activity in Ireland.

There may also be data protection issues and general contractual issues that need to be addressed, irrespective of the nature of the loans being traded.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Investment funds are authorised and regulated by the Central Bank and may be regulated as:

- undertakings for collective investment in transferable securities (UCITS) in accordance with the European Communities (Undertakings for Collective Investment in Transferable Securities) Regulations 2011, which implement the UCITS Directives into Irish law, and the Central Bank (Supervision and Enforcement) Act 2013 (Section 48(1)) (Undertakings for Collective Investment in Transferable Securities) Regulations 2019 (collectively the UCITS Regulations); or
- retail investor alternative investment funds (RIAIFs) or qualifying investor alternative investment funds (QIAIFs) in accordance with the requirements of the Central Bank and of the European Union (Alternative Investment Fund Managers) Regulations 2013 (as amended) (the AIFM Regulations), which implement Directive 2011/61/EU (Alternative Investment Fund Managers Directive) (AIFMD) into Irish law.

UCITS, RIAIFs and QIAIFs may be organised through a number of legal structures, the most popular of which are the Irish collective asset-management vehicle (ICAV), the investment public limited company (the investment company) and authorised unit trusts. It is an offence to carry on business as an ICAV, investment company or authorised unit trust unless authorised by the Central Bank.

Fintech companies, whether providing alternative finance products or otherwise, would not typically fall to be regulated as investment funds. However, fintech firms that fall within the definition of alternative investment funds would require authorisation. Fintech companies that provide services to investment funds may require authorisation if they are providing regulated depositary or administration services. Depositaries and administrators to investment funds may also engage fintech firms, in which case applicable Central Bank outsourcing requirements may apply, although in general, the fintech service providers would not themselves require authorisation.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

The Central Bank authorises and regulates Irish alternative investment fund managers (AIFMs) under the AIFM Regulations, as well as regulating UCITS management companies in accordance with the UCITS Regulations, and non-UCITS management companies (a residual category post-AIFMD). Most fintech companies would be expected to fall outside the scope of the AIFM Regulations and the UCITS Regulations.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

There is currently no distinct regulatory regime for peer-to-peer (P2P) or marketplace lending in Ireland. Some of the regimes described in this chapter (eg, retail credit and Regulation (EU) 2020/1503 (the Crowdfunding Regulation)) may, however, be relevant depending on the nature of the specific activities engaged in and a regulatory analysis of the proposed process flow is therefore always advisable.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

The Crowdfunding Regulation and Directive (EU) 2020/1504 (the MiFID 2 Amending Directive) were recently published to provide a common EU legislative framework in respect of crowdfunding.

The Crowdfunding Regulation became directly effective in Ireland in November 2021, and Ireland has implemented the MiFID 2 Amending Directive into national law. European crowdfunding service providers (ECSPs) are excluded from MiFID 2 by the MiFID2I Amending Directive, and ECSPs are instead covered by the Crowdfunding Regulation.

The Crowdfunding Regulation applies to P2P crowdfunding platforms facilitating business funding (lending to consumers is excluded) and investment-based crowdfunding platforms in relation to transferable securities up to a threshold of €5 million, whereas MiFID 2 will continue to apply to larger crowdfunding platforms.

Prospective ECSPs must apply for authorisation under the Crowdfunding Regulation and may avail of the ability to passport their licence into each of the EEA member states once approved. The Crowdfunding Regulation also places tailored operational and conduct of business requirements on ECSPs in their interactions with investors.

Invoice trading

11 Describe any specific regulation of invoice trading in your jurisdiction.

Holding title to loans advanced to consumers and SMEs can constitute 'credit servicing' requiring licensing under the Central Bank Act 1997 in certain circumstances. At a conduct-of-business level, the Central Bank (Supervision and Enforcement) Act 2013 (Section 48) (Lending to Small and Medium-Sized Enterprises) Regulations 2015 apply to regulated financial services providers and regulate the provision of credit by a regulated entity to micro and SME enterprises in Ireland. 'Credit' is broadly defined as a deferred payment, cash loan or other similar financial accommodation, including hire purchase, invoice discounting and the letting of goods. There are no regulations specific to invoice trading, described as such, in Ireland.

Payment services

12 Are payment services regulated in your jurisdiction?

Yes. The provision of payment services is a regulated activity requiring authorisation under the European Union (Payment Services) Regulations 2018 (the PSD Regulations), which transpose Directive (EU) 2015/2366 (revised Payment Services Directive) (PSD2) into Irish law. Ireland's implementation of the PSD2 through the PSD Regulations was consistent with the principle of maximum harmonisation, and as such the PSD Regulations reflect the requirements of the PSD2 itself.

Where PSD2 does not apply, there is a domestic regime under Part V of the Central Bank Act 1997, which regulates the 'money transmission business'. A money transmission business is defined as a business that comprises or includes providing a money transmission service to members of the public.

A proposed text of a PSD3 Directive is due to be published by the EU Commission in the second quarter of 2023 and may lead to further revisions to the regulatory perimeter in Irish law.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

Yes. One of the main aims of PSD2 was to increase competition in the payment sector, introduce open banking and facilitate access by third-party providers to a user's account held with their account servicing payment service provider (usually a bank). The Strong Customer Authentication requirements came into effect in September 2019, and this has required account servicing payment service providers to develop and test APIs to facilitate open access by third-party providers.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

There is currently no specific regulatory regime in place for robo-advisers or other companies that provide retail customers with automated access to investment products in Ireland.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Any entity that carries on insurance or reinsurance business in Ireland (namely, an insurance or reinsurance underwriter) requires an authorisation in accordance with the requirements

of Directive 2009/138/EC (Solvency II) as implemented in Ireland by the European Union (Insurance and Reinsurance) Regulations 2015.

The European Union (Insurance Distribution) Regulations 2018 (the IDD Regulations) came into force on 1 October 2018, and transpose Directive (EU) 2016/97 (Insurance Distribution Directive) into Irish law. The IDD Regulations set out authorisation and ongoing regulatory requirements for any person engaged in 'insurance distribution' in Ireland. This is broadly defined to include advising on, proposing, or carrying out other work preparatory to the conclusion of contracts of insurance, of concluding such contracts, or of assisting in the administration and performance of such contracts. Any fintech firm that sells or markets insurance products in Ireland (as a broker or agent) is likely to require authorisation in accordance with the IDD Regulations.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

The provision of third-party credit referencing or credit information services is not specifically regulated in Ireland, but historically this activity has not been widespread – credit checking was conducted directly by lenders themselves. Reflecting the fragmented credit information formerly available in Ireland, the Credit Reporting Act 2013 and associated regulations provide for the establishment and operation of a statutory central credit register (CCR) system, established and operated by the Central Bank. Credit providers in Ireland are required to provide information to the Central Bank for entry to the CCR and are also obliged to make an enquiry in respect of relevant credit applications.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

Yes, where the regulated activity is covered by relevant EU legislation, the provider is authorised in another EU or EEA member state and subject to compliance with the applicable notification procedures under relevant legislation.

As a general principle, where a financial institution authorised in another EU or EEA member state (the home state) passports its services into Ireland through the establishment of a branch in Ireland, or by providing its services on a cross-border services basis, the home state regulator retains responsibility for the prudential supervision of that entity. The regulator of the member state into which passporting is undertaken (the host state), in this case, the Central Bank of Ireland (the Central Bank), will supervise the passported entity's conduct of business in Ireland. The Central Bank does not in general adopt a gold-plating approach, and in general local conduct of business rules are not excessively onerous.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

Where a fintech company wishes to provide a regulated service, then, subject to the ability to passport into Ireland on a services basis where the fintech company is authorised in another EU or EEA member state, it is not possible to provide regulated financial services in Ireland unless the fintech company establishes a presence in Ireland.

The Central Bank, as the regulatory body responsible for authorising firms providing regulated financial services in Ireland, applies minimum substance requirements depending on the nature, scale, complexity and risk profile of the firm and the proposed activities and customers.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

There is no cross-industry financial promotions regime under Irish law and the promotion, sale and marketing of particular financial services and products are governed by sector-specific requirements, for example, under the European Union (Insurance Distribution) Regulations 2018, the Central Bank of Ireland's (the Central Bank) Consumer Protection Code 2012 and associated addenda or the European Union (Markets in Financial Instruments) Regulations 2017. These regimes set out rules in relation to offering financial services and products, disclosure and transparency requirements for advertising and rules relating to incentives for the sale of financial products and services to customers in Ireland, among other matters.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

There are no specific rules governing the use of distributed ledger technology or blockchain in Ireland, but a regulated financial service provider would need to comply with applicable conduct and regulatory requirements in applying such technologies to its regulated activities. The Central Bank of Ireland (the Central Bank) has issued a discussion paper relating to the impact of such innovation on its Consumer Protection Code and the delivery of financial services to consumers in Ireland.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

Virtual asset service providers (VASPs) are subject to a new registration obligation with the Central Bank for anti-money laundering and counter-terrorist financing purposes following Directive (EU) 2018/843 (Fifth Anti-Money Laundering Directive). Assuming the cryptoassets are not 'financial instruments' or other forms of collective investment, there is no regulatory framework governing cryptoassets in Ireland outside of the current AML framework.

However, there are plans ahead at the EU level for a regulation in Markets in Crypto-Assets (MiCA), which is similar to Directive 2014/65/EU (Markets in Financial Instruments Directive II) (MiFID 2), and this legislative proposal will develop a more suitable regulatory framework for virtual asset service providers across Europe, including passporting rights for those firms. MiCA has recently been finalised at the EU level and the Irish Department of Finance is expected to issue a consultation in the coming months on how certain aspects of it will be transposed into Irish law (such as the transitional authorisation regime for VASPs wishing to avail of MiCA).

We expect many of the Irish firms already providing virtual asset services will undergo this new domestic Irish authorisation process so that their operating models and compliance frameworks are robust enough to be able to then obtain authorisation as a cryptoasset service provider whenever the EU's MiCA legislation is finalised.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Assuming the digital currency in question is not considered a 'financial instrument' under MiFID and the exchange is not engaging in any other regulated activity, then there is no specific regulatory framework governing the operation of digital currency exchanges or brokerages in Ireland.

However, digital currency exchanges are considered VASPs under Irish AML legislation and VASPs with a physical establishment in Ireland are required to register with the Central Bank for AML supervision purposes only. It is expected that the MiCA regulation, when finalised, will provide a more comprehensive regulatory regime for digital currency exchanges and brokerages in the coming years.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

There are no specific rules governing the use of artificial intelligence (AI), including in relation to robo-advice, in Ireland. However, a regulated financial service provider would need to comply with applicable conduct and regulatory requirements in applying artificial intelligence (and robo-advice) to its regulated activities and would also need to ensure that it complies with Irish equality legislation (the Equal Status Acts 2000–2015) when using such technology to determine access to services. The Central Bank of Ireland (the Central Bank) has issued a discussion paper relating to the impact of such innovation on its Central Bank's Consumer Protection Code 2012 (the CPC) and associated addenda and the delivery of financial services to consumers in Ireland.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Most regulated businesses operating in Ireland are subject to change of control regimes that require direct and indirect acquisitions and disposals of qualifying holdings (10 per cent or more) to be notified to the relevant competent authority. For firms authorised in Ireland, the notification is made to the Central Bank of Ireland (the Central Bank), which then has a specific time period to review the change of control and request further information, confirm no objection, or object to the change. For credit institutions, the European Central Bank also has a role in the assessment of change of control notifications.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

The Criminal Justice (Corruption Offences) Act 2018 overhauled Irish anti-corruption laws and introduced a number of new offences, including a corporate liability offence that allows for a corporate body to be held liable for the corrupt actions committed for its benefit by any director, manager, secretary, employee, agent or subsidiary. The single defence available is demonstrating that the company took all reasonable steps and exercised all due diligence to avoid the offence being committed. Many firms are now implementing robust procedures and delivering training to staff on anti-bribery and corruption rules as a result.

Read this article on Lexology

Any fintech company that is a 'designated body' for the purposes of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (CJA) will be subject to anti-money laundering (AML) and counter-terrorist financing (CTF) requirements. Certain entities that are designated bodies for the purposes of the CJA, such as leasing companies, or those providing factoring services, do not require authorisations or licences from the Central Bank of Ireland (the Central Bank), but are subject to AML and CTF obligations under the CJA and are required to register with the Central Bank for that purpose. Fintech providers that are not regulated should therefore check on a case-by-case basis whether they are subject to the CJA.

Directive (EU) 2018/843 (Fifth Anti-Money Laundering Directive) has also been transposed into Irish law and a registration obligation for all firms acting as virtual asset service providers (VASPs) in Ireland has been in force since April 2021. Notably, because the legal framework is based on the EU's AML directives (and not Directive (EU) 2015/2366 (revised Payment Services Directive)), firms registered under this framework will not be able to passport their licences across the European Economic Area.

In addition to sector-specific requirements, fintech businesses may need to comply with consumer protection legislation (depending on the nature of the customers), Central Bank conduct rules, anti-money laundering requirements and data protection legislation.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is nothing specific to fintech companies. In line with other regulators, the Central Bank has generally increased its focus on AML, CFT and cyber risks across all regulated financial services. The Central Bank issued best practice guidance on cybersecurity within the investment firm and fund services industry in September 2015, followed by cross-industry guidance on information technology and cybersecurity risks in September 2016. The Central Bank will also expect relevant firms to apply European Banking Authority guidelines and technical standards published under Directive (EU) 2015/2366 (revised Payment Services Directive) and other specific regimes, as applicable. In June 2021, the Central Bank issued AML and CFT guidelines for the financial sector, to assist both credit and financial institutions in understanding their AML and CFT obligations as 'designated persons' under the CJA. These guidelines do not constitute secondary legislation but set out the expectations of the Central Bank regarding the factors that firms should take into account when identifying, assessing and managing ML and TF risks.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR) has had effect in Ireland since 25 May 2018 and is supplemented by the Data Protection Act 2018. The GDPR is intended to harmonise further the data protection regimes within the European Union and a full account of its impact is outside the scope of this chapter. For fintech operators, anonymisation and aggregation of data for commercial gain may be important. Aggregation of data for commercial gain will only be permissible where the collection, aggregation and commercial use of the data meets GDPR requirements. There may be somewhat greater flexibility in the use of anonymised data for commercial gain. However, it is generally accepted that the standard required for data to be truly anonymised (and therefore not be personal data) is a high one and that anonymisation techniques can only provide privacy guarantees if appropriate techniques are used and the application of those techniques is engineered appropriately. This is a complex area and any fintech operator considering engaging in such techniques should seek appropriate specialist advice.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

The Central Bank of Ireland (the Central Bank) issued best practice guidance on cyber-security within the investment firm and fund services industry in September 2015, followed by cross-industry guidance on information technology and cybersecurity risks in September 2016. The Central Bank will also expect relevant firms to apply relevant European Supervisory Guidelines, whether issued by the European Banking Authority or the European Supervisory Market Authority (such as the guidelines on security measures for operational and security risks under Directive (EU) 2015/2366 (revised Payment Services Directive) and other specific regimes, as applicable). The forthcoming EU Digital Operational Resilience Act will also be relevant here from 2025 onwards.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

There are multiple sector-specific requirements governing outsourcing, for example, under Directive 2014/65/EU (Markets in Financial Instruments Directive II) and Directive 2009/138/EC (Solvency II) regimes. For credit institutions, payments and e-money firms, the European Banking Authority (EBA) has issued extensive Guidelines as of February 2019. The Central Bank of Ireland (the Central Bank) takes an active interest in compliance by regulated firms

with outsourcing requirements and in November 2018, published the paper 'Outsourcing – Findings and Issues for Discussion', highlighting the most obvious and minimum supervisory expectations for regulated firms around the management of outsourcing risks. More recently, in December 2021, the Central Bank published Cross-Industry Guidance on Outsourcing and Cross-Industry Guidance on Operational Resilience.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

The Revised EBA Guidelines on Outsourcing (2019) are relevant here. In December 2021, the Central Bank of Ireland also published finalised Cross-Industry Guidance on Outsourcing and Cross-Industry Guidance on Operational Resilience, both of which are relevant to how financial services firms use and rely on cloud computing services in the course of their operational activities.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

The principal intellectual property right that protects software is copyright (the right to prevent others from, among other things, copying the software). Under the Copyright Act 2000 (as amended), copyright vests in the author on creation. Organisations should ensure that they have appropriate copyright assignment provisions in place in all agreements they have with employees or contractors to ensure that they obtain these rights.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

The default position under Irish law is that the employer owns intellectual property developed by an employee during the course of employment, unless it is otherwise stated in an agreement with the employee. However, this default position does not extend to intellectual property generated by an employee outside their employment (such as out of hours or off premises).

Contractors and consultants (who are not employees) are generally not subject to the default position described above and, unless the agreement between the contractor or consultant includes an assignment or other transfer of intellectual property to the customer, the contractor or consultant will own any intellectual property rights generated during the course of the work. Ownership of such intellectual property, if related to the subject matter of employment, should be addressed through the relevant contract.

Read this article on Lexology

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Yes. Joint owners of patents cannot assign or grant a licence of an interest in a patent or a design right without the consent of all other joint owners. Under the Trade Marks Act 1996 (as amended), a joint owner may sue another joint owner for trademark infringement where the trademark is used in relation to goods or services for which all joint owners have not been connected in the course of trade. On the basis of this legislation, we would expect that the consent of all joint owners is required for a licence of the trademark to be given.

Although the Copyright Act 2000 (as amended) is silent as to the rights of joint copyright owners, the current common law position appears to suggest that the consent of all co-owners is required for the grant of a licence to third parties.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

The European Union (Protection of Trade Secrets) Regulations 2018 (the Regulations) transpose Directive 2016/43 (Trade Secrets Directive) into Irish law and provide for civil redress measures in respect of the unlawful acquisition, use and disclosure of trade secrets. Prior to the operation of the Regulations, confidential information was protected either through a contractual agreement to keep certain information confidential or through the common law obligation to keep information confidential (because of the nature of the relationship between the discloser and disclose, the nature of the communication or the nature of the information itself).

The Regulations set out the circumstances in which the acquisition of a trade secret is considered lawful (eg, where the information is obtained by independent discovery) and also the circumstances in which the acquisition of a trade secret, without the consent of the trade secret holder, is considered unlawful (eg, by unauthorised access to, appropriation of, or copying of documents or materials etc).

The Regulations further provide that in legal proceedings relating to the unlawful, use or disclosure of a trade secret, the court may make an order directing that one or more relevant persons shall not be permitted to disclose or use any trade secret or alleged trade secret which has been identified as confidential.

There is no general rule, however, that requires confidential information that is revealed during court proceedings to be kept secret. It is possible to obtain an order from a court limiting access to such confidential information, but such orders are given on a case-by-case basis.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

The main intellectual property rights available to protect branding are registered and unregistered trade and service marks.

Registered trade and service mark rights only arise through registration and can be applied for either in Ireland (in respect of Ireland only) or more broadly in the European Union (as an EU trademark) or internationally. Trade and service mark rights give registered owners certain rights to prevent others from using identical or confusingly similar trademarks to their registered mark.

Brand owners can also rely on unregistered trademark rights through the common law of passing off. This allows the owner to prevent others from damaging their goodwill with customers by using branding or get-up that is identical or confusingly similar to their own.

For certain branding (particularly complex branding with artistic elements), copyright protection may also be available.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

The exact remedies available to individuals or companies depend on the intellectual property right that has been infringed. Generally speaking, however, for infringements of trademarks, patents, copyright and design rights under Irish law, the owner of the right may seek an injunction against further infringement, damages, an account of any profit made by the infringer from any articles incorporating the infringed intellectual property and delivery up or destruction of those articles.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

There are no competition issues in Ireland that are specific to fintech companies, nor do we expect that there will be any specific competition issues in the future.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

In addition to the Irish corporation tax rate of 12.5 per cent, there are a number of further Irish tax provisions that encourage innovation and investment in fintech in Ireland, including:

- A 25 per cent tax credit for qualifying research and development (R&D) expenditure carried on within the European Economic Area. This tax credit is in addition to the normal business deduction for such R&D expenditure (at the 12.5 per cent rate), thus providing relief for expenditure on R&D at an effective rate of 37.5 per cent. These credits may also be surrendered by the company to key employees actively involved in R&D activities, thereby reducing the effective rate of Irish income tax for such employees.
- A best-in-class 'knowledge development box', which complies with the Organisation for Economic Co-operation and Development's (OECD) 'modified nexus' standard. This can reduce the rate of Irish corporation tax to 6.25 per cent for profits derived from certain intellectual property assets, where qualifying R&D activity is carried on in Ireland. This relief can also be claimed in conjunction with the R&D tax credit.
- Tax depreciation for certain intangible assets. Such assets can be amortised for Irish corporation tax purposes either in line with their accounting treatment or on a straight basis over 15 years.
- The Employment and Investment Incentive and Start-up Refunds for Entrepreneurs schemes that allow individual investors in fintech companies to obtain Irish income tax relief (of up to 41 per cent) on investments made, in each tax year, into certified qualifying companies.
- Entrepreneur relief, which allows for a capital gains tax rate of 10 per cent on the disposal of certain qualifying business assets up to a lifetime amount of €1 million.
- An extensive double tax treaty network, totalling some 73 treaties, that prevents the taxation of the same portion of a company's income by multiple jurisdictions.
- Start-up relief, which provides for a reduction in corporation tax liability for the first three years of trading for certain size companies provided the company was incorporated on or after 14 October 2008 and began trading between 1 January 2009 and 31 December 2021. This relief can be claimed on both profits from trading and on capital gains.
- A stamp duty exemption for transfers of intellectual property.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

There are currently no proposals at the Irish national level to significantly increase tax or administrative costs for fintech companies in Ireland, though it should be noted that Ireland's corporation tax is set to rise from 12.5 per cent to 15 per cent as part of an OECD global deal on corporate tax reform that will set a minimum rate of 15 per cent for large companies. The expectation is that this will be implemented sometime during 2023.

Read this article on Lexology

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

There are no specific immigration schemes available for fintech businesses, or the technology and financial sectors, in Ireland. The ordinary rules in relation to employment permit requirements apply.

UPDATE AND TRENDS

Current developments

41 Are there any other current developments or emerging trends to note?

We expect Ireland to continue to develop as a leading domicile in this area. While we also expect the Central Bank of Ireland (the Central Bank) to follow best EU practice in its regulation of the sector and to adopt a relatively accommodating approach to fintech innovation, we do not necessarily expect the Central Bank to introduce a specific sandbox regime in Ireland.

Matheson

Ian O'Mara ian.o'mara@matheson.com
Joe Beashel joe.beashel@matheson.com

70 Sir John Rogerson's Quay, Dublin D02 R296, Ireland
Tel: +353 1 232 2000
www.matheson.com

Read more from this firm on Lexology

Read this article on Lexology

Italy

Benedetta Noro, Gabriella Rubino, Guendalina Catti de Gasperi, Marco Graziani and Marco D'Agostini*

Legance

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 304

General innovation climate 304
Government and regulatory support 305

FINANCIAL REGULATION 306

Regulatory bodies 306
Regulated activities 306
Consumer lending 307
Secondary market loan trading 307
Collective investment schemes 307
Alternative investment funds 308
Peer-to-peer and marketplace lending 309
Crowdfunding 309
Invoice trading 310
Payment services 310
Open banking 310
Robo-advice 311
Insurance products 311
Credit references 312

CROSS-BORDER REGULATION 312

Passporting 312
Requirement for a local presence 313

SALES AND MARKETING 313

Restrictions 313

CRYPTOASSETS AND TOKENS 313

Distributed ledger technology 313
Cryptoassets 314
Token issuance 314

ARTIFICIAL INTELLIGENCE 315

Artificial intelligence 315

CHANGE OF CONTROL 315

Notification and consent 315

FINANCIAL CRIME 315

Read this article on Lexology

Anti-bribery and anti-money laundering procedures 315
Guidance 316

DATA PROTECTION AND CYBERSECURITY 316
Data protection 316
Cybersecurity 317

OUTSOURCING AND CLOUD COMPUTING 317
Outsourcing 317
Cloud computing 318

INTELLECTUAL PROPERTY RIGHTS 319
IP protection for software 319
IP developed by employees and contractors 319
Joint ownership 320
Trade secrets 321
Branding 321
Remedies for infringement of IP 322

COMPETITION 323
Sector-specific issues 323

TAX 324
Incentives 324
Increased tax burden 326

IMMIGRATION 327
Sector-specific schemes 327

UPDATE AND TRENDS 328
Current developments 328

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

In recent years, attention in Italy towards fintech regulation has increased significantly. In particular, 2023 saw:

- the publication of Legislative Decree No. 30/2023, implementing Regulation (EU) 2020/1503 (Crowdfunding Regulation), and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937; and
- the publication of Law Decree No. 25/2023, which provides for urgent measures on the issuance and circulation of certain financial instruments in digital form and the simplification of fintech experimentation.

Further, it should be noted that on 17 May 2023, the Bank of Italy published consultation guidelines on crowdfunding service providers for businesses to provide modalities by

Read this article on Lexology

which these entities should comply with the provisions on corporate governance, internal controls, assessment of the suitability of natural persons responsible for their management and due diligence on project owners, the Crowdfunding Regulation, and related delegated regulations.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

In recent years, the Italian supervisory authorities have implemented several projects with the aim of facilitating discussions between operators and the authorities themselves.

In particular, with the aim of improving its capacity to analyse developments in the financial markets, the Bank of Italy has opened up a new channel of dialogue – the FinTech Channel – with operators who would like to propose innovative technological and organisational solutions in the financial services area, to make the Italian market more attractive.

The Italian Companies and Exchanges Commission (Consob) has also implemented the CONSOB-TECH initiative dedicated to companies and (or) individuals who have a project to develop technological innovations in the financial sector (fintech). In addition, LIFTECH is Consob's dedicated channel for discussion that aims to provide support for fintech companies and operators to move more easily through the complex regulatory and supervisory legal framework.

In this context, the Fintech Committee was established at the Ministry of Economy and Finance, composed of the Economy and Finance Ministry, the Ministry of Economic Development, the Ministry of European Affairs, the Bank of Italy, Consob, the Institute for the Supervision of Insurance, the Competition Authority, the Data Protection Authority, the Digital Italy Agency, and the Tax Agency. The Fintech Committee has the task to identify the objectives, define the programmes and implement actions to promote the development of techno-finance.

Subsequently, Ministerial Decree No. 100/2021, implementing Decree-Law No. 34 of 30 April 2019, introduced a regulatory sandbox through which the authorities observe the dynamics of technological development and identify the most appropriate legislative measures to promote and develop fintech (including insurtech), thus reducing the spreading of potential risks associated with these activities.

Operators can test innovative products and services, while benefiting from a transitional simplified regime. Where necessary, they can be granted regulatory exemptions during the testing phase, such as, for example, obtaining authorisation from the competent authority to carry out a regulated activity, in constant dialogue and confrontation with authorities.

Another initiative put in place by the Bank of Italy is the setting up of Milano Hub. Milano Hub is the innovation centre set up by the Bank of Italy on 21 July 2021 to support the digital evolution of the financial market and promote the attraction of talent and investment.

Read this article on Lexology

Milano Hub supports the development of innovative projects and research activities; it coexists with the Bank of Italy's Fintech Channel, a space for dialogue with operators, and with the regulatory sandbox, dedicated to experimentation activities assisted by supervisory authorities. Specifically, on 17 May 2023, a list of 14 eligible projects related to the artificial intelligence area was published and the support phase for their implementation by Milano Hub was then started.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

As of today, there are no specific provisions for fintech products and services; accordingly, the supervision of the provision of fintech products and services is not assigned to a single supervisory authority in Italy.

The Bank of Italy, the Italian Companies and Exchanges Commission (Consob) and the Institute for the Supervision of Insurance are equally competent depending on the fintech products being related to banking, finance or insurance sector.

Notwithstanding the above, note that aforementioned Legislative Decree No. 30/2023 identified the Bank of Italy and Consob as national competent authorities under Regulation (EU) 2020/1503 (Crowdfunding Regulation) on European crowdfunding service providers for business.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Reserved activities in Italy include the following:

- all types of financing to the public at large (including, among others, factoring, leasing, and assignment of credits) according to articles 10 and 106 of Legislative Decree No. 385/1993 (the Italian Banking Act) (IBA);
- taking deposits from the public at large according to article 10 of the IBA;
- payment services according to article 114-sexies of the IBA;
- collective asset management according to article 32-quarter of Legislative Decree No. 58/1998 (the Italian Financial Act) (IFA);
- investment services (eg, portfolio management services, dealing on own account in financial instruments, advising on investments) according to article 18 of the IFA;
- financial agency (namely, promotion and placement of banking products and payment services) according to article 128-quater of the IBA; and
- selling and (or) marketing of insurance products according to articles 11, 57 and 108 of Legislative Decree No 209/2005 (the Italian Insurance Act).

Consumer lending

5 Is consumer lending regulated in your jurisdiction?

Yes, professional consumer lending with respect to the public at large is regulated in Itlay. In particular, consumer lending activity is a reserved activity that only banks, Italian financial intermediaries enrolled in the register held by the Bank of Italy pursuant to article 106 of the IBA and foreign financial intermediaries not eligible for an EU passport provided that they are duly authorised by the Bank of Italy, are entitled to carry out.

The main provisions governing consumer lending are set forth by the IBA and in the corresponding implementing provisions relating to banking transparency as well as in Legislative Decree No. 206 of 2005 (the Consumer Code). Depending on the type of lending, some sectoral provisions apply; for example, some specific provisions apply only to real estate credit and others to salary-backed loans.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

The assignment of loans represents a type of financing; thus, the performance of this activity in Italy is reserved for authorised entities if it is carried out to the public at large according to articles 10 and 106 of the Italian Banking Act.

According to the Ministerial Decree No. 53/2015, the granting of credits is performed to the public at large if it is carried out regarding an undefined number of third parties and in a professional manner (namely, not on an occasional basis and relying on a dedicated organisation).

In general terms, the issuing of loans to the public at large could be performed by banks (pursuant to article 10 of the Italian Banking Act) and Italian financial intermediaries duly authorised by the Bank of Italy according to article 106 of the Italian Banking Act. As an exception to said general rule, some laws allow other entities to provide financing regarding the public at large, such as:

- credit funds, which may provide financing directly or purchase credits from other entities under article 46-bis of the IFA; and
- securitisation vehicles, to which Law No. 130/1999 allows for the purchase of credits from the originator of securitisation transactions.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

According to article 32-quarter of the IFA, the provision of collective asset management activities is reserved for Italian management companies (SGRs), EU management companies, EU

and third countries' alternative investment fund managers, open-ended investment companies (SICAV) and closed-ended investment companies (SICAF). Thus, the performance of the said activity requires the prior authorisation of the Bank of Italy (for SGR, SICAV, SICAF and third countries' alternative investment fund managers) or the completion of the passporting procedure (for EU management companies and EU alternative investment fund managers).

The collective asset management activity is qualified by the following features:

- the independence of the management company;
- the activity of collecting savings from third parties; and
- the existence of a predetermined investment policy.

The management of equity and lending crowdfunding platforms does not generally qualify as a collective asset management activity.

The EU Crowdfunding Regulation – in force from November 2021 – allows the crowdfunding platform managers to provide the individual portfolio management of loans service, namely the service of allocating by the crowdfunding service provider of a pre-determined amount of funds of an investor, which is an original lender, to one or multiple crowdfunding projects on its crowdfunding platform in accordance with an individual mandate given by the investor on a discretionary investor-by-investor basis. The provision of said service requires the platform manager to comply with the obligations under article 6 of the Crowdfunding Regulation, including, inter alia:

- the adoption of robust internal processes and methodologies;
- the keeping of records of the mandates given by clients and of every loan in an individual portfolio; and
- the assessment of the credit risk of individual crowdfunding projects selected for the investor's portfolio, the credit risk at the investor's portfolio level and the credit risk of the project owners selected for the investor's portfolio.

The provision of the individual portfolio management of loans service does not require the platform manager to be authorised for the performance of collective asset management activities or the provision of investment services. It will be sufficient if the platform manager is authorised to carry out crowdfunding services under article 12 of the Crowdfunding Regulation.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

Yes, the management of alternative investment funds represents a regulated activity in Italy.

According to article 34 of the IFA and the Regulation on Collective Asset Management issued by the Bank of Italy on 19 January 2015, the Bank of Italy, after consulting Consob, authorises the asset management companies to provide the collective asset management service for alternative investment funds. The asset management companies are registered on a list held by the Bank of Italy and are supervised by Consob and the Bank of Italy.

It is worth specifying that the status of a company as a fintech does not exempt such company from the application of asset management provisions.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

The EU Crowdfunding Regulation aims to foster cross-border funding of businesses by addressing the obstacles to the functioning of the internal market in crowdfunding services.

According to article 12 of the Crowdfunding Regulation, the manager of a crowdfunding platform (whether it is an equity or lending crowdfunding platform) must be authorised by the competent supervisory authority.

On 24 March 2023, Legislative Decree No. 30/2023 was published in the Official Gazette to adapt national legislation to the provisions of the Crowdfunding Regulation**.**

Legislative Decree No. 30/2023 amended the IFA to implement the Crowdfunding Regulation. More specifically, Legislative Decree No. 30/2023 introduces ex novo in the IFA:

- the definition of 'crowdfunding services', which replaces the previous definition of a 'capital raising portal for small and medium-sized enterprises and social enterprises' and directly refers to article 2(1)(a) of the Crowdfunding Regulation, thus covering the four forms of crowdfunding (equity, lending, donation and reward crowdfunding);
- identification of the Bank of Italy and Consob as national competent authorities under the Crowdfunding Regulation;
- regulations on crowdfunding offerings; and
- the regime of administrative sanctions on the subject of crowdfunding services.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

Specific rules on equity crowdfunding – the business funding model that allows innovative start-ups to raise capital through online portals from the crowd in exchange for a financial stake in the company – are included in the IFA. Italy was the first European country to adopt a specific regulation on equity crowdfunding (namely, Consob Regulation No. 18592/2013; the Consob Regulation whose provisions are no longer in effect because they have been replaced by those of the Crowdfunding Regulation).

According to the IFA and the Crowdfunding Regulation, a crowdfunding service provider must be authorised by Consob. On the other hand banks, payment institutions, e-money institutions and financial intermediaries must be authorised by the Bank of Italy. The European Securities and Markets Authorities should establish a public and up-to-date register of all crowdfunding service providers authorised in accordance with the Crowdfunding Regulation. That register should include information on all operating crowdfunding platforms in the European Union.

Read this article on Lexology

Invoice trading

11 Describe any specific regulation of invoice trading in your jurisdiction.

Invoice trading in Italy falls under the factoring discipline, as provided for by Law No. 52 of 21 February 1991. Factoring is a contract by which a company assigns its existing or future receivables to a specialised company, the factor, to obtain immediate liquidity and a range of services related to the management and the collection of the assigned receivables.

Since factoring is a reserved activity, it can be performed by banks (pursuant to article 10 of the IBA) and Italian financial intermediaries duly authorised by the Bank of Italy according to article 106 of the IBA.

Payment services

12 Are payment services regulated in your jurisdiction?

Yes, the performance of any payment services is reserved for banks, payment institutions and e-money institutions.

European provisions have impacted the Italian legal framework regarding payment services. In particular, reference is made to Directive (EU) 2015/2366 (revised Payment Services Directive) (PSD2). At the national level, the principal sources are:

- the IBA;
- Legislative Decree No. 11/2010; and
- the Bank of Italy Supervisory Regulation of Payment Institutions and Electronic Money Institutions of 23 July 2019.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

According to article 5-ter (regarding the payment initiation service (PIS)) and article 5-quarter (regarding the account information service (AIS)) of Legislative Decree No. 11/2010 and Commission Delegated Regulation (EU) 2018/389 supplementing PSD2, each financial institution providing payment accounts that are accessible online should offer at least one access interface enabling secure communication with PIS and (or) AIS service providers. The interface should enable PIS and (or) AIS service providers to identify themselves to the financial institution providing payment accounts. Such interfaces should also allow PIS and (or) AIS service providers to rely on the authentication procedures provided by the payment account service provider to the payment service user. To ensure technology and business-model neutrality, the payment account service providers should be free to decide whether to offer an interface that is dedicated to communication with PIS and AIS service providers, or to allow, for that communication, the use of the interface used by the payment account service providers for the identification and communication with the account users.

Read this article on Lexology

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

There are different kinds of robo-advice:

- pure robo-advice (namely, fully automated advice);
- hybrid robo-advice (namely, advice in which the manual and digital elements are combined, usually involving the possibility for the client to request the support of an adviser while using the digital platform); and
- robo for adviser (namely, financial advice in which the computer system works alongside the intermediary to optimise his or her advisory activities but in which the computer system does not interface with the consumer directly).

In Italy, along the lines of what is provided at the European level by Directive 2014/65/EU (Markets in Financial Instruments Directive II), which has expressly provided that the investment advice service can also be provided through automated or semi-automated systems, clarifying that the same provisions apply regardless of the channel of interaction with the investor, pure robo advice and hybrid robo advice can be considered within the scope of the investment advice service.

In fact, at both the EU and national levels, it has not been deemed necessary, at least for now, to proceed with the issuance of a differentiated regulatory legal framework or to change the definition of the advisory service. Robo for adviser, on the other hand, is not the subject of specific regulation.

The entities authorised to provide automated advice are generally: investment firms, banks, management companies, financial advisers and financial advisory firms that could also offer the independent financial advice service on an automated basis.

That said, there are specific provisions relating to behaviour and organisation that licensed entities must observe in pre-contractual negotiations, contract conclusion and provisions on client profiling, including the provisions relating to the marketing of financial services to consumers set forth by the Italian Consumer Code.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

The selling or marketing of insurance products is reserved activities according to articles 11, 57 and 108 of the Italian Insurance Act, even if they are carried out by fintech. The insurance distribution activity may be performed by:

- the insurance or reinsurance undertakings and their employees where they pursue this business directly;

- professional intermediaries (namely, agents, brokers, banks, investment firms, financial intermediaries and Poste Italiane SpA); and
- non-professional intermediaries (namely, ancillary insurance intermediaries whose principal professional activity is something other than insurance distribution).

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Yes, in Italy there are some restrictions on providing credit references or credit information services.

The credit reference represents the reputation that the client has with banks and financial intermediaries and reflects the correctness of its behaviour in the context of financing relationships. Verification of customers' credit references in Italy is carried out by credit information systems – once known as private risk data centres – these are the private databases consulted by banks and financial institutions to verify reliability and punctuality of payments and are used to assess the appropriateness of granting loans.

The credit information service is managed centrally by a legal person, entity or association; any relevant information is accessed only by those who voluntarily join and report it. The activity of private credit information systems is governed by Regulation (EU) 2016/679 (General Data Protection Regulation), Legislative Decree No. 196 of 30 June 2003 (the Privacy Code), and, more specifically, the Code of Ethics implementing the Privacy Code. The Code of Ethics was signed by private credit information systems managers, representatives of financial institutions, some consumer associations and the Data Protection Authority.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

Yes, regulated activities may be passported into our jurisdiction. For example, each EU bank authorised to conduct banking business in its EU home country may establish branches or conduct business under the freedom to provide services regime in Italy, subject only to prior notification to its national competent supervisory authority, which will forward such notification to the European Central Bank and the Bank of Italy.

Likewise, EU payment and e-money institutions may establish branches or conduct business under the freedom to provide services regime in Italy following a notification from the EU home country's competent supervisory authority to the Bank of Italy pursuant to article 114-decies and article 114-quinquies of the Legislative Decree No. 385/1993 (the Italian Banking Act) (IBA).

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

Yes, EU fintech companies may provide financial services without a branch in Italy. On this point, for instance, payment institutions and e-money institutions intending to provide payment services and issue e-money in an EU member state other than their home EU nation under the freedom to provide services shall notify their national competent supervisory authority.

Once the Bank of Italy has received the notification from the national competent supervisory authority, the EU payment institution is allowed to provide its services in Italy.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

The sale and marketing of financial products and services is a regulated activity that can be carried out by certain categories of entities, depending on the specific product or service to be sold or marketed.

For example, banks, financial intermediaries entered in the register provided for in article 106 of Legislative Decree No. 385/1993 (the Italian Banking Act) and investment firms are authorised to sell and market financial products or services. Further, the marketing of undertakings for collective investment units or shares is also a reserved activity that can only be carried out by certain entities such as asset management companies, EU management companies, open-ended investment companies, closed-ended investment companies and EU and non-EU alternative investment fund managers.

Similarly, the sales and marketing of insured products is reserved for, among others, insurance or reinsurance companies and intermediaries registered in sections (a) to (e) of the register held by the Institute for the Supervision of Insurance.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

On 17 March 2023, Law Decree No. 25/2023 was published in the Official Gazette. Law Decree No. 25/2023 provides for a pilot regime for market infrastructures based on distributed ledger technology (DLT) (DLT Pilot Regime) and the simplification of fintech experimentation.

Read this article on Lexology

In particular, Law Decree No. 25/2013 allows the issuance and transfer of digital financial instruments through registrations in the registers for digital circulation kept by a responsible party. The registration attributes to the party in whose favour it is made the full and exclusive entitlement to exercise the rights relating to the digital financial instruments.

When the registration in the register is made in favour of a bank or an investment firm acting in its own name and on behalf of one or more clients, the full and exclusive entitlement to exercise the rights follows the registration in the settlement account opened by the client with the intermediary and, in such a case, the restrictions on the digital financial instruments are constituted exclusively by the registrations in the relevant account.

If the issuance of digital financial instruments is not registered in the distribution settlement system (SS DLT) or a DLT trading system (TSS DLT), the transfer of the registrations from one register to another or the change of the circulation regime of the instruments is done by associating a public transfer strategy with them.

Each issuance is registered in only one register for digital circulation and each register is associated with a single responsible party. The issuance of digital financial instruments that are not registered with SS DLT or TSS DLT systems is also permitted only on special registers kept by responsible parties registered in the special list (including inter alia banks).

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

In Italy, there are no specific provisions regarding the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs).

If, however, cryptoassets are considered equivalents of financial instruments, the respective provisions of Legislative Decree No. 58/1998 (the Italian Financial Act) (IFA) apply.

The regulatory treatment of cryptocurrencies and cryptocurrency exchanges in Italy is likely to change dramatically in the future as a result of the forthcoming adoption of the EU Regulation on Markets in Cryptoassets (MiCA) (MiCAR), aimed at developing an EU-wide sound legal framework regulating all cryptoassets that are not covered by existing financial services legislation. On 20 April 2023, the European Parliament approved the text of the new MiCAR, which has been adopted by the Council on 16 May 2023. MICAR is expected to come into force before the end of 2023.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Although the issuance and marketing of tokens is under the supervision of the Italian Companies and Exchanges Commission (Consob), there is still no regulation of ICOs, STOs

or other token generation events. While waiting for MICAR to come into effect, when the ICO has as its object a cryptoasset that can be qualified as a financial instrument, the relevant provisions on public offerings of financial instruments set forth by the IFA will apply. This would imply, inter alia, the obligation for the issuing company to disclose a prospectus, subject to Consob approval.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

There are no specific provisions for artificial intelligence, although see under the heading 'Robo-advice'.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Under the Italian regulatory framework, transactions entailing the acquisition of a controlling shareholding of an Italian-regulated entity are subject to the prior authorisation of the relevant supervisory authority, including the European Central Bank in the case of a bank's change of control.

The authorisation is granted when certain conditions to ensure the sound and prudent management of the regulated entity is met, including, among others, the quality of the potential acquirer (namely, the fulfilment of honourability, professionalism and integrity requirements) and its financial soundness, the quality of the future members of the corporate bodies of the regulated entities and the suitability of the business plan of the regulated entity.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Yes, fintech companies provide services functional to the use, exchange, and storage of virtual currency and their conversion from or into currencies as well as providers of digital wallet services (services for the safeguarding of private cryptographic keys on behalf of clients to hold, store and transfer virtual currencies) are among those obliged to adopt the

Read this article on Lexology

anti-money laundering measures provided for in Legislative Decree No. 231 of 2007. These entities must also have objective and consistent procedures, for the analysis and assessment of money laundering and terrorist financing risks. In assessing the risk of money laundering or terrorist financing, obliged entities take into account risk factors associated with the type of customers, geographic area of operation, distribution channels, and the products and services offered.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

Presently, there is no regulatory or industry anti-financial crime guidance for fintech companies.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

Ordinary data protection rules (namely, Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR), and Legislative Decree No. 196 of 2003 of the Italian Privacy Act) apply to transfers of personal data in the fintech sector. This means that any communication of fintech-related data between controllers – being those in or outside the European Union – shall take place only when a legal basis under the GDPR exists (eg, users' consent, the necessity to execute a contract with the users, discharge of legal obligations etc). For international data transfers, GDPR rules apply, therefore, any envisaged transfer shall be preceded by a transfer impact assessment and, if the recipient is not located in a white-listed country, the transfer shall either rely on adequate safeguards (article 46 of the GDPR) or a valid derogation for the specific situation (eg, specific data subject's consent, etc (see article 49 of the GDPR)).

When it comes to the exchange of consumer credit information within the country among financial and credit entities, it is worth mentioning the Code of Conduct for Information Systems Operated by Private Entities on Consumer Credit, Reliability and Punctuality of Payments, adopted in 2019 by the Italian Data Protection Authority. Practically, this Code of Conduct sets the privacy regulatory framework for setting up and managing private credit bureaus. The Code contains detailed provisions on the type of data that can be inserted into the database, the data retention periods, the security measures that shall be applied by the database managers, as well as interesting provisions on the scoring of consumers: in this regard, for example, it provides that financial scoring can only take place in the context of existing or requested loans, and can be performed only by the company that received the loan request or the one that first introduced the borrower's data in the database; besides, the statistic models and algorithms underpinning the scoring shall be periodically reviewed to avoid the risk of biased decisions, which would affect the borrower's legal sphere.

Read this article on Lexology

Even though fintech promises to disrupt the credit market by overpassing the logic of the credit bureaus, the Code of Conduct is a useful example of co-regulation with some good hints also for real-time financial assessments taking place in the fintech domain.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

From a cybersecurity point of view, fintech business is highly impacted by the security standards set out by Directive (EU) 2015/2366 (revised Payment Services Directive) (PSD2) and the related EU and Italian legislation implementing it. In some instances, fintech actors, as providers of essential services, are included in the scope of application of Directive 2022/2555/EU (Network and Information Systems Directive II) (NIS2), which, repealing Directive (EU) 2016/1148 (Network and Information Systems Directive), requires to implement detailed risk management measures and to report cybersecurity incidents to the national competent authorities.

In light of the developed EU cyber framework, some of the fintech actors may have assets included in the National Cybersecurity Perimeter: this means that they may be subject to stringent security standards set out by the regulators (such as, among the many, asset inventory, business continuity plans, incident notification obligations, controls over the supply chain, etc).

Further, on 14 December 2022, the European Parliament and the Council of European Union adopted Regulation (EU) 2022/2554 Regulation 2022/2554/EU on digital operational resilience for the financial sector, which lays down uniform requirements concerning the security of network and information systems (ICT) supporting the business processes of financial entities.

Last, the European Commission has recently proposed a regulation (Cyber Resilience Act) to impose specific obligations on the economic operators, in relation to the cyber security of the products with digital elements (meaning any software or hardware product and its remote data processing solutions), which are used also in the contest of the fintech business.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Yes, companies providing financial services may outsource certain functions of their business, in accordance with the applicable regulations. Such outsourcing of essential or important functions is permissible in compliance with the principle of proportionality but, in any event, the responsibility of the regulated company remains intact.

Generally speaking, the outsourcing of critical or important functions requires the prior notice to the competent supervisory authorities.

By way of example, banks should notify the European Central Bank or the Bank of Italy before outsourcing the critical or important functions. An institution, therefore, shall notify the Bank of Italy at least 60 days before the outsourcing takes effect where the institution intends to outsource operational functions related to:

- payment services;
- the issuance of electronic money;
- the system of internal control;
- the information system; or
- critical components.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

The use of cloud computing by banks, payment institutions and electronic money institutions is regulated within the EBA Guidelines on outsourcing arrangement (EBA/GL/2019/02) that repealed the previous EBA's recommendation on outsourcing to cloud service providers. Within the new guidelines there are specific provisions related to the outsourcing to cloud service providers such as those related to the obligation to include in the register of the outsourcing arrangements, the cloud service and deployment models (namely, public-private-hybrid community), and the specific nature of the data to be held and the locations (namely, countries or regions) where such data will be stored.

The use of cloud computing by investment firms, on the other hand, is regulated by the Guidelines on Outsourcing to Cloud Service Providers (the Guidelines) issued by the European Securities and Markets Authority. By way of example, the Guidelines require that inter alia:

- the parties' respective rights and obligations shall be clearly defined in a written agreement;
- information security requirements shall be set in the internal policies and procedures; and
- exit strategies shall avoid undue disruption to the business activities and services to the clients.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Under Italian law, software is mainly protected by copyright. Article 2, No. 8 of Law No. 633 of 22 April 1941 on copyright protection (as further amended), affords copyright protection to computer programs, in whatever form expressed, and to their preparatory design materials.

Copyright on software is obtained with the sole creation of the work. No registration requirement is set under Italian law. Software may (but this is not a mandatory requirement) be filed with the Italian Company of Authors and Publishers to obtain a preferential evidence of the paternity and date of existence of the software, for certainty of proof.

Software-implemented inventions are also eligible for patent protection, under article 45, paragraphs 2 and 3, of Italian Legislative Decree No. 30 of 10 February 2005 (Industrial Property Code) (IPC), provided that they implement inventions.

Business models, as such, are not eligible for patent protection, pursuant to article 45, paragraph 2(b) of the IPC. Yet, if the business model consists of a process meeting the requirements for patent protection (novelty, inventive step and industrial application) there might be room to obtain patent protection.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Employees' inventions are regulated under article 64 of the IPC, which provides for the following three different cases.

Service inventions

If an employee has been hired specifically to perform an inventive activity and he or she receives a specific remuneration for such activity, the employer owns any right to the inventions developed, while the employee will only be recognised as the author of the inventions and will not be entitled to any further award or payment.

Company inventions

If an employee has not been hired specifically to perform an inventive activity and (or) he or she has not been granted with a specific remuneration for this purpose, but he or she develops certain inventions in the execution of the employment contract and using the equipment and instruments of the employer, the latter will own any right to the inventions developed and the employee will be recognised as the author of the inventions. In addition, the employee will be entitled to a fair award.

Read this article on Lexology

Occasional inventions

If the invention is developed by an employee outside the scope of the employment, by using his or her own equipment and instruments, but falls within the field of activity of the employer, the latter holds an option right to use the invention, or to purchase the subsequently patented invention, as well as the right to file or purchase, for the same invention, patents in foreign territories; the employee shall be entitled to a payment of a price (whose amount shall be determined considering the invention's market and the possible contribution of the employer) and shall, in any case, be recognised as the author of the invention.

With respect to freelance workers, article 4 of Law No. 81/2017 has provided that the IP rights in inventions or works developed by freelance workers in the performance of their duties vest in the employer whether the inventive or creative activity is:

- expressly provided for; and
- specifically remunerated in the relevant agreement.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Pursuant to article 6 of the IPC, unless written agreements are entered into between the joint owners, the rules of the Italian Civil Code on joint ownership apply.

article 6 of the IPC also expressly provides for the right of each co-owner to file applications or renew registrations, prosecute applications, pay annual fees, translate patent claims, regardless of the consent of the others.

In general terms, the basic principle of the Italian Civil Code on joint ownership is that each of the co-owners may use the co-owned (intangible) good provided that:

- the destination of use of the good is not altered; and
- his or her use does not prejudice the right of use of the other co-owners.

As to the administration of the co-owned good, co-owners have a vote right, depending on their shares. Different majorities are necessary for acts of ordinary or extraordinary administration.

As to assignment and charge (such as pledge), the consent of all co-owners is necessary.

Regarding licenses, a line must be drawn between exclusive and nonexclusive licenses. For nonexclusive licenses, a simple majority of the co-owners is needed, since they are considered acts of ordinary administration. On the other hand, a two-thirds majority is needed for exclusive licenses.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Trade secrets are protected under articles 98 and 99 IPC.

In particular, under article 98 IPC protection is afforded to business information and technical-industrial experience, including commercial information and experience, subject to the legitimate control of the owner, provided that they:

- are confidential (namely, not generally known or easily accessible for experts and operators in the field);
- have an economic value inasmuch as it is confidential; and
- have been subject, by their owner, to measures that may be deemed reasonable to keep them secret.

Adequate measures shall be of a technical (segregation of information, efficient passwords, etc) and legal nature. Indeed, with regard to trade secrets protection, it is essential to enter into appropriate contractual arrangements. A company can protect its trade secrets by entering into non-disclosure agreements with potential clients, contractors or investors before providing them with any confidential information. It can also have confidentiality, non-competition or non-solicitation, exclusivity and intellectual property clauses in the agreements with its employees. Likewise, the company can implement an enforceable data security policy, which will, among other things, restrict access to relevant business information to a need-to-know basis.

The owner is entitled to an exclusive right, meaning that he or she has the right to prohibit third parties from acquiring, disclosing to third parties or using that information and experience in an unauthorised manner, except for cases in which the third party has obtained it in an independent manner by the third party.

Trade secrets are also protected in court. Article 121-ter of the IPC provides that the judge, in the course of the proceedings, may prevent all subjects not expressly authorised, including parties, legal counsels, witnesses and clerks, from having access to confidential information. Further, the judge may forbid the people appointed or delegated by him or her, the parties and their representatives and consultants and witnesses, from using or disclosing the trade secrets that are the subject of the proceedings that he or she deems confidential.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Fintech brands can be protected by registering the trademarks of the relevant business entity, for the classes of goods and services of interest (usually, core services fall within class 36 of the Nice Agreement for the registration of trademarks). It is advisable to secure registration for the trademark under which the business operates, as well as for the brand

of the core products or services offered on the marketplace, if different. In addition, It is advisable to secure registration of the domain names of interest.

Italian law also protects non-registered trademarks, if used. The scope of protection, both from a geographical and goods or services standpoint, depends on the extension of use. If the non-registered trademark is used with a not merely local significance (namely, on the entire territory of Italy), it causes the invalidity of subsequent identical or confusingly similar trademarks. Obversely, the non-registered trademark will coexist with the later registered trademark. In general terms, non-registered trademarks are more difficult to enforce and filing is always advisable.

Unfair competition can also be invoked to protect brands.

Fintech companies may reduce the risk of infringing third parties' trademark rights by performing clearance searches before adopting or launching new trademarks. The search is performed in the official trademark registers and has the scope to disclose the existence of earlier identical or confusingly similar trademarks, adopted by third parties for identical or similar goods and services. The mentioned clearance searches do not disclose the existence of unregistered trademark rights. For this reason, it is advisable to also perform a market search in the business field of interest to identify trademarks used de facto by third parties.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

The owner of an IP right is entitled to act against any third party who is infringing its right, to obtain the court to convict the defendant and inflict on him or her the sanctions provided by law.

To obtain a prompt outcome and contain damages, the IPC provides for special ad interim measures, and in particular, inter alia, for search orders, injunction, seizure and withdrawal from the market.

An injunction, on the other hand, is the order by which the court prevents the infringer from carrying on activities that infringe on someone else's IP right. An injunction may be granted ante causam or ongoing.

With regard to the products made through the infringing activity and the tools specifically and exclusively used for the purpose of infringement, the court may order their destruction and seizure at the counterfeiter's expense.

In addition, upon a party's motion, the judgment may order the publication of the judgment at the expense of the infringer, in newspapers and magazines.

Italian IPC also allows the right to order the definitive withdrawal of infringing products from the market. This ad interim measure is different from the injunction and requires a duty of

cooperation so that the prejudice to the infringed IP right ceases by removing the infringing products from the market.

In addition, the owner of the IP right can seek compensation for damages, as part of a merits proceedings.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

Competition and consumer protection issues, which involve also fintech companies, have arisen in the recent past in Italy.

The Annual Law for the Market and Competition in Italy crucially introduced important amendments to the Italian Antitrust Law (Law No. 287/1990) and other provisions, by strengthening the competence of the Italian Competition Authority, broadening the scope of its jurisdiction as well as its investigative powers with regard to merger control, anti-trust and abuse of economic dependence. Notably, the criteria to calculate the turnover of banking and financial institutions for merger control purposes has been revised and are now aligned with those of the European Union. The change results in the relevant turnover being calculated on the basis of the income deriving from operations that reflect the scope of the activity carried out by the bank or financial institution, as opposed to its asset value. As a result, the turnover of assets free fintech companies could be significantly higher than the turnover resulting from the application of the previous criterion. Also, with the aim of tackling killer acquisitions in the digital and technological sector, the Italian Antitrust Law now allows the Italian Competition Authority to review transactions that are below the turnover thresholds if certain conditions are met. Last, the provision on abuse of economic dependence has been reinforced, with the introduction of a rebuttable presumption of economic dependence from digital platforms and an indicative list of practices in which such abuse can materialise.

In 2022, several investigations in the financial and banking sector were closed by the Italian Competition Authority. For instance, in October 2022, the Italian Competition Authority closed the abuse of dominance investigation into Mastercard's conduct concerning contactless payments by accepting and making binding commitments. The investigative hypothesis was that Mastercard's double-tap mandate could have constituted an abuse of its dominant position, in such a way as to exclude Bancomat's, also in relation to its access to e-wallets on major smartphones. Mastercard offered a set of commitments, including to define technical indications of the double-tap mandate as guidelines with no binding effect, to leave the market free to decide how to set up point-of-sale terminals. In addition, in November 2022, the Italian Competition Authority closed its investigation into a project aimed at modifying the remuneration model for automatic teller machine withdrawals from banks other than one's own using Bancomat network cards. According to the Italian Competition Authority, the new remuneration model would have resulted in a restriction of competition to the detriment of consumers.

Read this article on Lexology

Further, the Italian Competition Authority, following the best practices of the European Commission and numerous national competition authorities, has introduced its own whistle-blowing platform so that whistle-blowers will be able to send information on anti-competitive conduct and the people involved through a platform on the Italian Competition Authority's website, while remaining anonymous.

On the consumer law side, the implementation of the Omnibus Directive has significantly amended the Italian Consumer Code (Legislative Decree 206/2005) and strengthened consumer rights in Italy, bringing in a broad range of changes such as information requirements in distance contracts between the trader and the consumer, application of certain rules of the Consumer Code to contracts where the consumer provides personal data as consideration, additional unfair practices, revised parameters for assessing misleading omissions, the increase of the maximum fine for unfair commercial practices to €10 million and new fines for infringements of EU relevance.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

The main tax incentives in Italy for fintech companies consist of the following.

Tax credit for research and development

All businesses entities tax resident in Italy, including permanent establishments of non-Italian resident entities, regardless of legal form, the economic sector to which they belong, the size and tax regime for determining their business income, investing in one of the eligible activities identified pursuant to Italian laws, may benefit from this tax benefit. The tax credit is granted in an amount equal to 20 per cent of certain eligible costs (net of other grants or contributions received for any reason), with an annual maximum limit of €4 million up to fiscal year 2022, and to 10 per cent of the eligible costs, with an annual maximum limit of €5 million from fiscal year 2023 and up to fiscal year 2031. Fundamental research, industrial research and experimental development in the scientific or technological field are considered research and development activities eligible for the tax credit.

Tax credit for technological innovation activities

All business entities tax resident in Italy, as described above, may benefit from this tax benefit. The tax credit is granted in an amount equal to 10 per cent of certain eligible costs (net of other grants or contributions received for any reason), with an annual maximum limit of €2 million up to fiscal year 2023, and to 5 per cent of the eligible costs with an annual maximum limit of €2 million from fiscal year 2024 and up to fiscal year 2025. Activities of technological innovation eligible for the tax credit are considered the ones, other than those of research and development, aimed at creating new or substantially improved products or production processes.

Read this article on Lexology

Patent box

Taxpayers realising business income may opt for this tax regime, consisting in increasing for income tax purposes by 110 per cent research and development costs incurred in relation to certain types of legally protectable intangible assets (eg, software protected by copyright, industrial patents, designs and models). The option has a duration of five fiscal years and is irrevocable and renewable.

For the purposes of the patent box, it is necessary that:

- the assets are used directly or indirectly in carrying out the relevant business activities; and
- taxpayers carry out research and development activities aimed at the creation and development of assets whose cost is increased for tax purposes also through research contracts, stipulated with companies other than those directly or indirectly controlling the business entity, which are controlled by this latter or are controlled by the same company that controls the business entity or with universities or research or equivalent bodies.

As for the investors' side, the main tax incentives are the ones directed to innovative start-ups as defined according to Italian laws (namely, set-up entities not more than 60 months old and not listed on the stock exchange), which are tax resident in Italy or an EU member state or in an EEA member state provided that the same have a production office or a branch in Italy and comply with specific requirements, including the one to have as exclusive or predominant corporate purpose the development, production and marketing of innovative products or services with high technological value.

Set out in more in detail, these tax incentives consist of the following.

Deduction of an amount equal to 30 per cent of the investment into an innovative start-up or innovative SME

This tax incentive allows for the deduction, from the gross personal income tax for Italian resident individuals (namely, a tax credit) and from the corporate income taxable base of Italian resident entities, of an amount equal to 30 per cent of the eligible investment in one or more innovative start-ups or small or medium-sized (SME) enterprises carried out directly or indirectly (namely, through companies or investment funds (including alternative investment funds)), which invest mainly into innovative start-ups or SMEs.

The maximum eligible investment (for which an incentive is given) cannot exceed, in each fiscal year, €1 million for Italian resident individuals and €1.8 million for Italian resident entities; the amount not fully deductible during the reference fiscal year may be brought forward, but not beyond the third following year. Moreover, the said investment must be held for at least three years.

Deduction of an amount equal to 50 per cent of the investment into an innovative start-up or innovative SME

This tax incentive allows to deduct from the gross personal income tax for Italian resident individuals only an amount equal to 50 per cent of the eligible investment in one or more innovative start-ups or SMEs carried out directly or indirectly (namely, through investment funds (and not through companies)), which invest mainly into innovative start-ups or SMEs. Moreover, the said incentive is granted pursuant to the de minimis EU Regulation (namely, Regulation (EU) No. 1407/2013)) and, therefore, the innovative start-up or the innovative SME recipient of the investment cannot obtain de minimis aid for more than €200,000 over three financial years. For accessing the incentive, a precise procedure should be complied with.

The maximum eligible investment (for which an incentive is given and which) cannot exceed, in each fiscal year, €100,000 for the investment into innovative start-ups and €300,000 for the investment into innovative SMEs. This tax incentive is an alternative to the tax deduction under the above in the case of investment into an innovative start-up, while it applies to the amount exceeding the €300,000 threshold of whether the investment is in an innovative SME. The eligible investment must also be held for at least three years.

Other tax incentives for directors, employees or continuous collaborators of the innovative start-up or SME and for equity

These tax incentives provide for an exemption from personal income taxes (and, in the case of financial instruments assigned to the directors, employees or continuous collaborators of the innovative start-up or SME, and also from social security contributions) of the income deriving from the assignment of financial instruments by the innovative start-up or SME, provided that certain conditions are met.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

The recent Digital Service Tax applies a 3 per cent rate on revenues deriving from:

- the supply of transmission services on a digital advertising interface aimed at users of the same interface;
- making available a multilateral digital interface, which allows users to be in contact and interact with each other, and also to facilitate the direct supply of goods or services; and
- the transmission of data collected from users and generated by the use of a digital interface.

Taxation, in practice, concerns digital advertising on websites and social networks, access to digital platforms, the fees received by the managers of these platforms, and the transmission of data taken by users.

Business operators subject to the payment of the Digital Service Tax are those who during the calendar year preceding the one in which the tax assumption arises:

- generate a total amount of revenues of no less than €750 million anywhere in the world, individually or jointly at the group level; or
- receive in the same period, individually or jointly at the group level, an amount of revenues from digital services of not less than €5.5 million in Italy.

The Italian Digital Service Tax is, however, transitory, meaning that it will be repealed with effect from the moment in which the provisions deriving from international agreements on the taxation of the digital economy come into force.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

To date, there are no specific immigration schemes available for fintech businesses to recruit skilled staff from abroad. Nonetheless, Italian and EU law provides some benefits of general character:

- Freedom of movement of workers who are EU citizens. EU law provides EU citizens the freedom of movement and residence to apply for a job and be treated on an equal footing with nationals of another EU country.
- EU Blue Card. The EU Blue Card can be issued to non-EU highly-qualified workers, giving them the right to live and work in an EU country, provided they have at least a three-year university degree and an employment contract or a binding job offer (with a minimum duration of one year) with a salary equal to at least €24,789.93 (in Italy). In Italy, such workers are not included in the numerical limits (quota) that are normally set by Italian authorities for the entry of foreign workers. By November 2023, upon the implementation of a recent EU Directive, the requirements for obtaining the EU Blue Card will be simplified; the minimum duration of the employment contract will be reduced to six months (instead of one year), while the new minimum annual salary will be determined by the Italian implementation law (between a minimum of €26,580 and a maximum of €42,528).
- A visa special treatment for digital nomads and remote workers who are non-EU citizens. Digital nomads and remote workers are defined as 'citizens of a third country who carry out highly qualified work activities through the use of technological tools that allow working remotely, autonomously or for a company based outside Italy'. They can apply for a one-year visa provided that they have full health insurance and that tax and social security obligations are met.
- A visa special treatment for non-EU investors. Non-EU investors who 'in their own name or on behalf of the legal entity they legally represent' intend to invest at least €250,000 in a start-up can apply for a visa of more than three months.
- Italia Startup Visa is a programme for entrepreneurs from non-EU countries who intend to create a start-up in Italy. The programme allows a simplified application procedure for a one-year visa for self-employment.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

Italian supervisory authorities are increasingly focusing their attention on fintech-related phenomena and this trend is also expected to increase in view of the upcoming EU Payment Services Directive III.

While Italian supervisory authorities are trying not to disincentivise such new services, in line with the global trend, their attention is also focused on the protection of small investors. The number of statements is growing in which supervisory authorities are warning investors of the high risks associated with cryptoassets (see most recently the Joint Statement of the Italian Companies and Exchanges Commission and the Bank of Italy of 28 April 2021).

In line with the need to preserve investors from the frauds and risks associated with cryptoassets, in Italy, in implementation of article 4 of the Decree of the Ministry of Economy and Finance of 13 January 2022, it was provided that there is the obligation for service providers related to the use of virtual currency and digital wallets to register in the special section of the exchange register kept by the Agents and Credit Brokers Body referred to in article 17 bis, paragraph 1 of Legislative Decree No. 141 of 13 August 2010.

It is also worth mentioning the growing trend of operators to use the new buy now, pay later (BNPL) form of credit. In this regard, it is worth noting the communication of 28 October 2022, in which the Bank of Italy, again with a view to protecting customers, clarified the provisions to be applied when using one BNPL scheme rather than another.

* *The authors wish to thank Lucio Scudiero, Noemi di Donato, Giacomo Poletti, Chiara Scala and Edoardo Canali for their assistance in the preparation of this chapter.*

Legance

Benedetta Noro	bnoro@legance.it
Gabriella Rubino	grubino@legance.it
Guendalina Catti de Gasperi	gcattidegasperi@legance.it
Marco Graziani	mgraziani@legance.it
Marco D'Agostini	mdagostini@legance.it

Via Di San Nicola Da Tolentino 67, Rome 00187, Italy
Tel: +39 06 93 18 271
www.legance.it

Read more from this firm on Lexology

Read this article on Lexology

Japan

Ken Kawai, Akihito Miyake, Yutaka Shimoo and Kensuke Inoue

Anderson Mōri & Tomotsune

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 330

General innovation climate 330
Government and regulatory support 331

FINANCIAL REGULATION 332

Regulatory bodies 332
Regulated activities 332
Consumer lending 333
Secondary market loan trading 333
Collective investment schemes 334
Alternative investment funds 334
Peer-to-peer and marketplace lending 334
Crowdfunding 335
Invoice trading 335
Payment services 335
Open banking 335
Robo-advice 336
Insurance products 336
Credit references 336

CROSS-BORDER REGULATION 337

Passporting 337
Requirement for a local presence 337

SALES AND MARKETING 337

Restrictions 337

CRYPTOASSETS AND TOKENS 338

Distributed ledger technology 338
Cryptoassets 338
Token issuance 339

ARTIFICIAL INTELLIGENCE 340

Artificial intelligence 340

CHANGE OF CONTROL 340

Notification and consent 340

Read this article on Lexology

FINANCIAL CRIME 340
Anti-bribery and anti-money laundering procedures 340
Guidance 341

DATA PROTECTION AND CYBERSECURITY 341
Data protection 341
Cybersecurity 342

OUTSOURCING AND CLOUD COMPUTING 343
Outsourcing 343
Cloud computing 343

INTELLECTUAL PROPERTY RIGHTS 343
IP protection for software 343
IP developed by employees and contractors 344
Joint ownership 344
Trade secrets 345
Branding 345
Remedies for infringement of IP 345

COMPETITION 346
Sector-specific issues 346

TAX 346
Incentives 346
Increased tax burden 347

IMMIGRATION 347
Sector-specific schemes 347

UPDATE AND TRENDS 348
Current developments 348

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

In Japan, fintech innovation has been quite active in almost every area of finance. In particular, cryptocurrency-based businesses, cashless payment or mobile payment services, financial account aggregation services, robo-advisers and crowdfunding are well known to the public.

Over the past 12 months, we have seen notable developments in the blockchain and web3 sector, including the non-fungible tokens' sector, the digital securities' sector and stable-coin services, despite of the turmoil in crypto-related businesses around the world.

Non-fungible token-related businesses have continued to be popular, especially in the online gaming sector. In addition, content holders, digital-art artists and advertising agencies have been active in this market.

Digital security businesses have been gaining stronger momentum. Their main focus is on digital corporate notes and tokenised equity interests of real estate funds.

In June 2022, the bill to amend the Payment Services Act and Banking Act has passed the Diet. One of the main purposes of the amendments is the introduction of a regulatory framework for issuers and intermediaries that handle stablecoins. The new regulations came into force on 1 June 2023.

The new regulatory regime for financial services intermediary businesses started on 1 November 2021, which enables service providers to act as an intermediary for cross-sectoral banking, securities and insurance financial services under a single licence. Over the past 18 months, seven service providers obtained such licenses and started the intermediary service.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Yes. Financial regulators and policymakers in Japan are supportive of fintech innovation and new technology-focused entrants in the regulated financial services markets. For instance, the Ministry of Economy, Trade and Industry has been supportive of the blockchain industry, and it hosted the Blockchain Hackathon in February 2019 as part of a broader effort for the social implementation of blockchain technologies.

In June 2018, the Japan Economic Revitalisation Bureau, under the auspices of the Cabinet Secretariat, opened a cross-government one-stop desk for the regulatory sandbox in Japan (the Regulatory Sandbox). The Regulatory Sandbox can be used by both Japanese and overseas companies, enabling them to apply and receive approval for projects, not yet covered by present laws and regulations, and to conduct demonstrations under certain conditions without the need for a legal amendment to cover the project.

Tokyo Metropolitan Government has established X-HUB Tokyo, a platform that connects Tokyo with the global innovation ecosystem and accelerates the startups that will open up a new era. Its Inbound Program aims to support overseas startup companies, including, fintech companies, in their expansion into Tokyo through the provision of opportunities to interact with Tokyo-based companies.

In early 2021, Osaka Prefectural Government established the Global Financial City OSAKA Promotion Committee to promote the city as a new international financial centre in Asia. The committee aims to realise an 'innovative financial region' through drastic deregulation in new financial technology fields such as fintech.

Since early 2022, the Japanese ruling party, Liberal Democratic Party (LDP), has been supporting web3 businesses in Japan. LDP Digital Society Promotion Headquarters web3 Project Team has issued three policy papers since then. The web3 White Paper (Toward an era of mass adoption of Digital Assets), issued in April 2023, mainly contains:

- issues to be addressed immediately for prompting web3; and,

Read this article on Lexology

- issues that should be further explored for the further development of web3.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

The Financial Services Agency (FSA) is the main regulatory body of fintech products and services that are regulated under various financial regulations. The Ministry of Economy, Trade and Industry is also the regulatory body for certain payment services (eg, credit cards or other advanced payment services).

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

The arrangement of investment deals for an investment fund that invests mainly in securities or derivative transactions, constitutes a 'financial instruments business' under the Financial Instruments and Exchange Act (FIEA), and registration under the FIEA is required.

To arrange transactions for investments that mainly comprise securities or derivatives, registration under the FIEA is also required.

Dealing in investments as principal or agent, under which investments are made mainly in securities or derivative transactions, may also constitute a financial instruments business under the FIEA (in certain circumstances); thus, registration under the FIEA may also be required.

Giving advice on investments in relation to the value of securities or investment decisions on financial instruments under a contract for a fee may constitute an 'investment advisory business' under the FIEA, and registration is required.

Lending money is regarded as a 'moneylending business', which generally requires registration as a moneylender under the Moneylending Business Act.

There is no specific licensing requirement for factoring transactions and invoice discounting.

Secondary market loan trading does not trigger a licensing requirement.

Acceptance of deposits is generally prohibited without a banking licence under the Banking Act.

There is no licensing requirement for foreign exchange transactions.

A bank licensed under the Banking Act may conduct funds transfer services (which will generally include payment services). Other than banks, registration under the Payment Services Act (PSA) as a funds transfer service provider is required before conducting

payment services. If the payment service is provided as a later payment option using a credit card, then registration under the Instalment Sales Act is required for the issuers.

Japan has specific regulations on cryptoassets (CAs) under the PSA. A company that provides its users with the following services is required to undergo registration as a Crypto Asset Exchange Services Provider:

- the sale and purchase of CAs in exchange for fiat currencies or the exchange of CAs for other CAs;
- intermediary, agency or delegation services in respect of the acts listed in item (1);
- management of customers' money in connection with the acts listed in items (1) and (2); or
- management of CAs for the benefit of another person (namely, a cryptoasset custody service).

Fiat-backed stablecoin regulations under the PSA came into force on 1 June 2023. Under the new regulations, a fiat-backed stablecoin is named as 'electronic payment instruments' (EPIs).

A banking licence or fund transfer business registration would in principle be required to issue EPIs. In addition, trust companies and foreign trust companies are also permitted to issue certain types of EPIs.

Moreover, a company that provides its users with the following services is required to undergo registration as an electronic payment instruments exchange service provider:

- sale and purchase of EPIs or exchange of EPIs for other EPIs;
- intermediary, brokerage or delegation activities in respect of such sale, purchase or exchange; and
- management of EPIs for the benefit of another person.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

A lender conducting consumer lending activities must register as a moneylender under the Moneylending Business Act. The total permissible lending amount is generally limited to one-third of the borrower's annual income if the borrower is an individual. The cap of the interest falls between 15 per cent and 20 per cent per annum depending on the principal amount of the loan pursuant to the Interest Rate Restriction Act.

Secondary market loan trading

6 | Are there restrictions on trading loans in the secondary market in your jurisdiction?

There is no specific licensing requirement for trading loans. If a moneylender transfers loan claims, the transferee will be subject to the same restrictions under the Moneylending

Business Act that are applicable to the original moneylender, and the transferor must notify the operating transferee of the applicability of the restrictions.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Under the FIEA, the solicitation of subscription of shares in collective investment schemes or investment management of assets of collective investment schemes, in principle, are regarded as financial instruments businesses. Therefore, business operators who conduct those activities must be registered as financial instruments business operators.

If a crowdfunding company raises funds for investment in a company through a form of a *tokumei kumiai* (TK) partnership, or if a social lending company raises funds for lending money to a company seeking funds through that form of partnership, the solicitation to invest in the partnership would, in principle, be considered as falling within the scope of a financial instruments business activity and must, thus, be registered under the FIEA.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

In Japan, there are no regulations that particularly focus on alternative investment fund managers. Under the FIEA, investment managers acting for alternative investment funds, such as hedge funds, private equity funds and real estate funds, are regulated in the same manner as those acting for investment funds similar to undertakings for the collective investment in transferable securities, which means they are not subject to the augmented regulations under the FIEA. However, additional licences may be required under other laws (apart from the FIEA) for such alternative investment fund managers who conduct the business of managing investors' funds by investing in real estate (not the beneficiary rights therein).

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Marketplace lending in Japan generally takes the form of a TK partnership, under which a social-lending business provider collects funds from TK partnership investors. The social-lending business provider advances the funds to enterprises or individuals as loans. The operator then receives principal and interest payments from the enterprises or individuals and distributes the funds as dividends and returns to investors. In this structure, the operator is required to be registered both as a moneylender under the Moneylending Business Act (to provide the loans) and as a financial services provider under the FIEA to solicit the purchase of interests in TK partnerships to investors.

Read this article on Lexology

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

In Japan, crowdfunding is categorised as donation-based crowdfunding, reward-based crowdfunding and investment-based crowdfunding. Investment-based crowdfunding is further categorised as equity-based crowdfunding, fund-based crowdfunding and social lending.

Reward-based crowdfunding involves a sales and purchase agreement of the reward. It is not regulated under the FIEA.

Equity-based crowdfunding and fund-based crowdfunding are regulated under the FIEA, which defines certain internet-based solicitations, such as 'electronic solicitation handling services'. Certain special provisions apply to electronic solicitation handling services compared with those that apply to ordinary solicitation handling services for securities.

Invoice trading

11 Describe any specific regulation of invoice trading in your jurisdiction.

There is no specific regulation that applies to invoice trading in Japan. If invoice trading is with recourse to a supplier (namely, the seller of the invoice) when no repayment is forthcoming from the buyer, those transactions may be characterised as secured lending, and the business would be required to obtain a moneylending business licence under the Moneylending Business Act.

Payment services

12 Are payment services regulated in your jurisdiction?

Payment services fall within the scope of funds remittance transactions, which generally require a banking licence under the Banking Act. The Payment Services Act permits non-banking entities registered thereunder to engage in funds remittance transactions in the course of their business, subject to certain restrictions. Pursuant to recent revisions to the Payment Services Act that came into effect on 1 May 2021, three types of fund transfer services have been established. Each of these fund transfer services is regulated differently, in terms of the permitted amount per transaction, fund retention and other matters relevant to customer protection.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

The Banking Act regulates electronic payment intermediate service providers in relation to the open application programming interface. Electronic payment intermediate service providers are defined to include intermediaries between financial institutions and

customers, such as entities using IT to communicate payment instructions to banks based on entrustment from customers, or entities using IT to provide customers with information about their financial accounts held by banks. Entities providing financial account aggregation services are also categorised as electronic payment intermediate service providers. They are required to register with the FSA.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

A robo-adviser that provides retail customers with automated access to investment products must be registered as an investment manager (if it provides discretionary investment management services) or an investment adviser (if it provides non-discretionary investment advisory services) under the FIEA. If the robo-adviser accepts the customers' assets, it must also be registered as a Type I financial instruments business operator under the FIEA.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Yes. In Japan, a company (including a fintech company) that conducts insurance solicitation (namely, acts as an agency or intermediary for insurance contracts) must be registered as an insurance agent or insurance broker under the Insurance Business Act. Further, under the Act on Provision of Financial Services (this being the proposed new name of the current Act on Sales, etc, of Financial Instruments), which will come into effect on 1 November 2021, a person who is registered to conduct financial services intermediary business may, as an insurance intermediary service, intermediate the conclusion of certain life insurance and non-life insurance contracts.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

In general, while credit references of individuals are subject to the Act on Protection of Personal Information, credit references of corporations are subject to confidentiality obligations under financial services regulations (such as the Corporate Information under the Moneylending Business Act) and confidentiality agreements between financial institutions and corporations.

In Japan, personal credit information agencies collect information on the ability of persons to make credit repayments and provide the information to financial institutions that are members of those agencies. Financial institutions (banks or moneylenders) may not use information on the ability of individuals to meet repayments (personal credit information) for purposes other than the investigation of the ability of fund users to make repayments.

Read this article on Lexology

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

In most cases, no.

Japan is a member of the Asia Region Funds Passport (ARFP), which allows for a fund to be 'exported' to another participating economy, provided that it complies with the regulations of the jurisdiction in which the fund is registered, the applicable regulations relating to the offer in the host jurisdiction and the ARFP passport rules.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

It depends on the nature of the services that the foreign fintech company intends to provide; however, generally speaking, foreign fintech companies will be required to have a subsidiary or a business office to obtain a licence under applicable laws.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Providers of financial products and services should pay attention not only to their respective regulating laws and regulations and the guidelines issued by their regulatory or self-regulatory bodies, but also to the general customer protection legislation, such as the Act against Unjustifiable Premiums and Misleading Representations, the Consumer Contract Act and the Act on Specified Commercial Transactions, when advertising, selling and marketing financial products and services.

In respect of investment products and services, such as securities, derivatives, 'deemed securities' (eg, limited partnership interests) and investment advisory and management services, only registered financial instruments business operators or financial institutions (FIBOs) are permitted to sell and market such investment products or services under the Financial Instruments and Exchange Act (FIEA). As a general rule, a FIBO is prohibited from soliciting investment products or services that are not suitable for an investor in light of his or her knowledge, experience, financial conditions and purpose of investment. A FIBO is required to deliver an explanatory document on the details of investment products or services to investors in advance.

In respect of insurance products, only insurance agents or brokers are permitted to sell and market insurance products for their affiliated insurance company under the Insurance

Business Act. As a general rule, an insurance company, agent or broker must provide information regarding insurance contracts to customers. An insurance company, agent or broker must understand each customer's intention, recommend and explain the insurance product meeting the customer's intention, and offer to the customer an opportunity to reconfirm whether the recommended product meets the customer's intention. The rules on advertising, sales and marketing of investment products and services under the FIEA apply mutatis mutandis in respect of variable annuity and insurance products and certain foreign currency-denominated insurance products.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

No.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

While the promotion or use of cryptoassets is not directly regulated, a service provider who deals with digital currencies or stablecoins, may be regulated as a cryptoasset exchange service provider, an electronic payment instruments exchange service provider, a prepaid payment instruments issuer or, as the case may be, a fund transfer service provider under the Payment Services Act (PSA).

On the other hand, a service provider who deals with NFTs will not be regulated under the PSA unless such service provider does not engage in a fund transfer service or such utility tokens or NFTs fall under cryptoassets, prepaid payment instruments or electronic payment instruments under the PSA.

A cryptoasset exchange service provider is defined as an entity that, as a business:

1 purchases, sells and exchanges cryptoassets;
2 acts as a broker, intermediary or agent with regard to the transactions listed in (1);
3 maintains users' money or cryptoassets in relation to the transactions listed in (1) or (2); or
4 holds cryptoassets in custody for and on behalf of another person, unless otherwise licensed to do so under the applicable laws.

A prepaid payment instruments issuer is a person who issues prepaid payment instruments for its own or a third party's business. To issue e-money, which falls within the definition of 'prepaid payment instruments for a third party's business', the issuer is required to undergo registration under the PSA.

Read this article on Lexology

Issuing digital currencies or fiat-backed stablecoins that are redeemable in cash constitutes a fund transfer service, which triggers a requirement to be licensed or registered under the Banking Act, the Payment Services Act or the Trust Business Act.

An electronic payment instruments service provider is defined as an entity that, as a business:

1 purchases, sells and exchanges electronic payment instruments;
2 acts as a broker, intermediary or agent with regard to the transactions listed in (1);
3 maintains users' electronic payment instruments, subject to certain exceptions; or
4 increase or decrease the balance of users' electronic payment instruments based on delegation by the fund transfer service provider who is an issuer of such electronic payment instruments.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Generally speaking, an STO that deals with security tokens that are regarded as securities is regulated under the Financial Instruments and Exchange Act (FIEA), while an ICO that deals with tokens that are regarded as cryptoassets, prepaid payment instruments or electronic payment instruments is regulated under the PSA.

It had not been clear whether STOs, ICOs or any other methods of token generation were governed by the PSA or the FIEA, or both. In 2020, the FIEA introduced the concept of electronically recorded transferable rights (ERTRs) to clarify the scope of tokens governed by the FIEA. The PSA clarifies that ERTRs do not fall under the category of 'cryptoassets' governed by the PSA.

Tokens generated in security token offerings will constitute ERTRs if they meet the three requirements of 'collective investment scheme interests' under the FIEA and are represented by proprietary value transferable by means of an electronic data processing system. Collective investment scheme interests are deemed to be formed if:

- investors contribute cash or other assets (including cryptoassets) to a business;
- the cash or other assets so contributed are invested in the business; and
- investors have the right to receive dividends of profits generated from investments in the business.

ERTRs may be subject to the disclosure rules under the FIEA. An offering of ERTRs will need to be handled by a Type I financial instruments business operator registered under the FIEA.

On the other hand, tokens that do not fall under the definition of ERTRs but are used as payment instruments are likely to constitute cryptoassets or prepaid payment instruments governed by the PSA.

Read this article on Lexology

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

No. A robo-adviser using artificial intelligence is regulated under the Financial Instruments and Exchange Act (FIEA), generally in the same way as an ordinary investment adviser or manager.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

A shareholder holding more than 5 per cent but less than 20 per cent of the voting rights held by all the bank's shareholders (a major holder of the bank's voting rights) must file a notification with the Financial Services Agency (FSA) within five business days. A shareholder who intends to hold, whether individually, jointly or as a group, 20 per cent or more of the voting rights (a bank's major shareholder) must obtain authorisation from the FSA in advance. Moreover, a bank's major shareholder holding more than 50 per cent may be ordered to submit the relevant bank's business improvement plan.

A shareholder of an insurance company is subject to substantially the same rules as those applicable to a major holder of a bank's voting rights and a bank's major shareholder, as outlined above.

A shareholder holding, in principle, 20 per cent or more of the voting rights held by all of the Type I financial instruments business operator's or investment manager's shareholders (a major shareholder) must file a notification with the competent local finance bureau without delay. A major shareholder who comes to hold 50 per cent or more of the voting rights (a specified major shareholder) must file a further notification without delay.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

A person who gives, or offers or promises to give, a bribe to a domestic or foreign public officer can be subject to a criminal penalty under the Criminal Code or, as the case may be, the Unfair Competition Prevention Act. Although fintech companies are not explicitly

required by law to put in place anti-bribery procedures, they are expected to do so as a part of their effective internal control.

The Act on Prevention of Transfer of Criminal Proceeds (APTCP) requires 'specified business operators' (most financial service providers are included therein) to:

- verify each customer's identity, the purpose of the transaction, occupation and, in the case of a corporate customer, the identity of its representatives and ultimate owners and its purpose of business;
- verify each customer's financial condition in the case of a high-risk transaction;
- create and keep a record of verification and transaction reports; and
- report any suspicious transaction to the competent authority.

A fintech company falling under a specified business operator is required to put in place anti-money laundering procedures under the APTCP and the Financial Services Agency's Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

No.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The Personal Information Protection Act (PIPA) applies to any person (or company) who processes and transfers personal data. General and industry-specific guidelines (including the financial services industry guideline) regarding the protection of personal information are issued by the Personal Information Protection Committee and the relevant government authority (including the Financial Services Agency (FSA)). However, the guidelines issued by the Committee and relevant government authorities do not focus in particular on the fintech industry.

The PIPA requires that any person who handles a personal information database in the course of business (a personal information handling business operator (PIHBO)) must, generally:

- not handle any personal information beyond the minimum scope necessary for achieving the purpose of use;
- not transfer any personal data to a third party without obtaining the prior consent of the relevant data subject;
- keep the personal data accurate and updated;

- put in place necessary and appropriate measures to store and handle the personal data in a safe manner;
- disclose all personal data held about a relevant data subject to that subject whenever requested; and
- correct, and delete or cease to use, any personal data they hold if the relevant data subject so requests with reasonable grounds (hereafter, collectively, the General Rules).

If personal data is transferred within Japan, as an exception to the General Rules, a PIHBO may transfer personal data (excluding sensitive personal information) to a third party without obtaining the prior consent of the relevant data subject. This is only if the PIHBO notifies the matters prescribed by the PIPA to the relevant data subject and the Personal Information Protection Committee. However, from April 2022, illegally acquired information and information acquired via this exception must be handled in accordance with the General Rules.

If personal data is to be transferred to a third party located overseas, a PIHBO must adhere to the following special rules:

- the PIHBO must obtain the relevant data subject's prior consent to the transfer of personal data to a third party located overseas;
- the relevant third party must be located in a jurisdiction that has an equivalent personal information protection framework to the PIPA; or
- the relevant third party must put in place equivalent personal information protection measures to those required of a PIHBO under the PIPA.

The General Rules do not apply in respect of anonymised data. Instead, the PIPA requires a PIHBO to comply with the standard prescribed by the PIPA and the relevant government guidelines when creating and handling anonymised data to ensure that it is impossible to identify any specific individual or extract personal information from that data. A person who handles anonymised data in the course of business must, when transferring it to a third party, notify the third party of the types of information relating to individuals contained within and clearly state that the information to be transferred remains anonymised.

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

A general regulation was introduced pursuant to the Basic Act on Cybersecurity in 2014. In addition, according to the upcoming policy for cybersecurity in the finance field, the FSA has strengthened its measures regarding cybersecurity.

In addition, the Centre for Financial Industry Information Systems publishes the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions (the FISC Guidelines). The FSA refers to the FISC Guidelines when inspecting and monitoring fintech business operators.

The FSA's inspection manuals and supervisory guidelines show points of focus in connection with cybersecurity risk management.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Broadly speaking, financial services companies may outsource a part of their business to a third party but are required, for those purposes, to put in place any necessary measures to ensure the outsourced business will be appropriately performed pursuant to the relevant laws and regulations. Such measures include, without limitation, the:

- selection of an appropriate service provider that is eligible to perform the outsourced business;
- monitoring and supervision of outsourced service provider's performance of duties; and
- replacing or ceasing to retain the outsourced service provider if it is found that the outsourced service provider does not appropriately perform its duties.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

No.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Software may be protected by copyright or patent, or as a trade secret.

Computer program software can be protected by copyright under the Copyright Act of Japan (the Copyright Act) as a 'work of computer programming' without the need to undergo any application procedure if the computer program has the requisite creativity.

Under the Patent Act of Japan (the Patent Act), if the information processing by the software is concretely realised by hardware, a patent for the software-implemented invention may be obtained by filing an application with the Japanese Patent Office. Business methods by themselves are not patentable, and must be tied to a computer or computer network systems to be eligible for patent protection.

If the software meets the requirements of a 'trade secret' under the Unfair Competition Prevention Act (UCPA), which is, in essence, that the software is non-public knowledge,

contains useful information and is kept secret, it may be protected as a trade secret without the need to file for registration.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Under article 15 of the Copyright Act, the employer is the author of any work created by an employee while performing his or her duties for the employer and that otherwise meets the legal requirements. Therefore, the copyright and moral rights to the work are retained by the employer as the author, unless separately agreed upon.

Under article 35 of the Patent Act, an invention made by an employee is deemed to be an 'employee invention' if it falls within the scope of the employer's business, and the act that led to the invention is part of the employee's current or past duties at the employer. If the employer has not established separate rules regarding the right to obtain a patent to an 'employee invention', the right will vest with the employee. If the employer has established rules that give ownership of the right to obtain a patent to 'employee inventions', the right will belong to the employer. In that case, the employee has a statutory right to receive reasonable compensation for the invention.

Independent contractors and consultants who are not employees are usually entitled to copyright and patent rights for works they create and inventions they develop, unless otherwise contractually agreed upon.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Under article 65 of the Copyright Act, if a work is created and each creator's contribution to the work cannot be separated and used individually, the copyright is held jointly. If one of the joint copyright holders wants to assign, license or use the work, he or she can only do so with the consent of all the other joint copyright holders. Under article 73 of the Patent Act, when a patent is held jointly, each of the joint holders may use the patent independently. However, the consent of the other joint patent holders is required for the assignment or license of the patent to a third party.

In the event of an infringement of copyright or patent rights, injunctive relief and claims for damages may be brought independently.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Trade secrets (including confidential information) can be protected by the Unfair Competition Prevention Act (UCPA). Under article 2, paragraph 6 of the UCPA, a protectable trade secret is defined as:

- production methods, sales methods, and other technical or business information useful for business activities;
- that are kept secret; and
- are not publicly known.

A court may, in a legal proceeding upon the motion of a party, issue a protective order, including prohibiting a party and its agents from disclosing the relevant trade secret to any other persons.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brands may be protected by a trademark under the Trademark Act of Japan (the Trademark Act. A trademark may be registered if an application is submitted to and approved by the Japan Patent Office. Applications can be submitted online. In addition, brands may be protected under article 2, paragraph 1, items 1 and 2 of the UCPA, regardless of whether or not they are registered, provided that it can be proven that the relevant product, or the product's indications, is well known or famous.

For fintech businesses to ensure that they do not infringe existing brands, they must conduct research on existing trademarks. They can utilise J-PlatPat, the database operated by the National Centre for Industrial Property Information and Trading, to conduct the initial screening.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

The holder of the intellectual property rights can claim actual damages arising from the infringement. As this is difficult to do in practice, the Patent Act, the Copyright Act, the Trademark Act and the UCPA each provide provisions that presume damages, such as reasonable royalties. The holder of intellectual property rights can also seek injunctions against infringing third parties, as well as actions required to prevent the infringement. In addition, they may seek relief to restore honour or credit. For example, under article 115 of the Copyright Act, a copyright holder may petition the court to issue an order compelling the

infringer to issue a public apology. Infringing third parties may also be subject to criminal penalties as provided under the respective statutes.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

In April 2020, the Japan Fair Trade Commission published fintech-related market research reports, including the Account Aggregation Service Report and the Cashless Payment Service Report, based on its extensive research through questionnaire surveys and hearing surveys.

The Account Aggregation Service Report found, among other things, that if a bank in a superior position unjustly refuses application programming interface access from an account aggregation service provider, then in light of normal business practice, the bank's conduct would be in violation of the Antimonopoly Act (AMA).

The Cashless Payment Report identified the following potential issues, among others:

- banks and fund transfer service providers are competitors in cashless payment, but such non-bank players must be connected to the user's bank account to provide their service. Accordingly, if a bank in a superior position unjustly refuses fund transfer service providers access, the bank's conduct would be in violation of the AMA;
- interbank settlement charges when using Zengin System, a nationwide online network system for banks, have been fixed at a high rate for many years. Banks must reconsider whether the level of the charges is reasonable; and
- at present, Zengin-Net, the Zengin System operator, does not allow fund transfer service providers to access Zengin System. Zengin-Net should set reasonable conditions for access by fund transfer service providers.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

There are no tax incentives specifically targeting fintech companies and investors. That being said, the Japanese tax system contains provisions for statutory angel investors who invest in statutory unlisted corporations that were incorporated within the past 10 years with the following tax incentives:

- at the time of investment:

- a reduction of income tax for investment in a target company that is less than five years old;
- a reduction in the capital gains from the transfer of shares for investment in a target company that is less than 10 years old; and

- at the time of sale of the shares in the target company:

  - the offset of capital losses against other capital gains and carryover of such losses for three years after the sale.

Following recent tax reforms, a tax incentive to promote open innovation was made available from April 2020 to the end of March 2024. Under these tax measures, an income deduction equivalent to 25 per cent of the investment amount will apply to investments of at least ¥100 million in unlisted venture companies that are generally less than 10 years old, by domestic entities and corporate venture capital that intends to hold shares of such companies for three years or more.

In addition, a research and development tax incentive system has been adopted and will be frequently revised with the aim of maintaining and strengthening initiatives that support Japan's global competitiveness.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

No.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

Foreign nationals recognised as 'highly skilled foreign professionals' will be given preferential immigration treatment. There are three categories of activities of highly skilled foreign professionals:

- advanced academic research activities;
- advanced specialised or technical activities; and
- advanced business management activities.

A person who is recognised as a highly-skilled foreign professional can enjoy preferential treatment, including permission for multiple purposes of activities and a grant of a five-year stay.

Read this article on Lexology

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

No.

ANDERSON MŌRI & TOMOTSUNE

Ken Kawai	ken.kawai@amt-law.com
Akihito Miyake	akihito.miyake@amt-law.com
Yutaka Shimoo	yutaka.shimoo@amt-law.com
Kensuke Inoue	kensuke.inoue@amt-law.com

1-1-1 Otemachi Otemachi Park Building,
Chiyoda-ku, Tokyo 100 8136, Japan
Tel: +81 3 6775 1000
www.amt-law.com

Read more from this firm on Lexology

Read this article on Lexology

Luxembourg

Cathrine Foldberg Møller, Julie Carbiener, Camille Saettel, Camille Bénézet and Maya Coumes
Simmons & Simmons

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 350
General innovation climate 350
Government and regulatory support 351

FINANCIAL REGULATION 352
Regulatory bodies 352
Regulated activities 352
Consumer lending 353
Secondary market loan trading 354
Collective investment schemes 354
Alternative investment funds 354
Peer-to-peer and marketplace lending 354
Crowdfunding 355
Invoice trading 355
Payment services 355
Open banking 356
Robo-advice 356
Insurance products 357
Credit references 357

CROSS-BORDER REGULATION 357
Passporting 357
Requirement for a local presence 358

SALES AND MARKETING 358
Restrictions 358

CRYPTOASSETS AND TOKENS 359
Distributed ledger technology 359
Cryptoassets 359
Token issuance 359

ARTIFICIAL INTELLIGENCE 360
Artificial intelligence 360

CHANGE OF CONTROL 360
Notification and consent 360

FINANCIAL CRIME 360

Read this article on Lexology

Anti-bribery and anti-money laundering procedures 360
Guidance 361

DATA PROTECTION AND CYBERSECURITY 361
Data protection 361
Cybersecurity 363

OUTSOURCING AND CLOUD COMPUTING 363
Outsourcing 363
Cloud computing 364

INTELLECTUAL PROPERTY RIGHTS 364
IP protection for software 364
IP developed by employees and contractors 364
Joint ownership 365
Trade secrets 365
Branding 366
Remedies for infringement of IP 366

COMPETITION 366
Sector-specific issues 366

TAX 367
Incentives 367
Increased tax burden 367

IMMIGRATION 368
Sector-specific schemes 368

UPDATE AND TRENDS 368
Current developments 368

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Luxembourg has a vibrant and rapidly growing fintech scene. The Grand Duchy hosts a large number of financial service providers, including a growing number of virtual asset service providers (currently there are 10 virtual asset service providers registered in Luxembourg). Several payment institutions and electronic money institutions have established their European financial hub in Luxembourg. An innovative local fintech start-up scene is developing digital tools to help companies and financial institutions. With Luxembourg being one of the leading investment fund centres in the world, the accumulation of fundtech providers comes as no surprise and the technology provided is being rapidly adopted by established institutions. Additionally, especially in the areas of payments, platforms, blockchain and related ancillary services, the regulatory landscape is rapidly growing and evolving and a vast number of fintech and fundtech providers are already active in the country.

Read this article on Lexology

The current boom shows no signs of slowing down as the Luxembourg government remains committed to attracting new start-ups and scaling up entrepreneurs and investors.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Overall, the Luxembourg financial sector is robust, largely thanks to its community of financial institutions and agile public institutions that have always been resilient in withstanding different crises.

The three official languages (Luxembourgish, French and German) make Luxembourg a diverse and dynamic global financial centre, where English is commonly used in the workplace. The Luxembourg Financial Sector Regulator (CSSF), is also able to work in English and also provides most of its publications, legislation and its guidelines in English.

To help fintech initiatives, the CSSF has created a dedicated innovation hub that intends to help with the regulatory challenges surrounding financial innovation and to foster a constructive dialogue between the regulator and actors of the financial sector. To do so, the CSSF has created a dedicated contact form for the innovation hub available in French and in English on the CSSF website.

To provide an agile and efficient regulatory environment for fintech companies, Luxembourg has been modernising its legislative framework since 2014 when crypto exchanges or platforms and the provision of payment services using virtual or other currencies were recognised as financial service providers and able to obtain a licence. Further in 2019, the possibility to issue dematerialised securities on distributed ledger technology was introduced by law. In 2021, the CSSF also published its guidance on virtual assets along with two frequently asked questions for undertakings for collective investments and credit institutions. A Luxembourg law implementing the EU's Distributed Ledger Technology (DLT) Pilot Regime in Luxembourg has been voted on and further strengthens the already advanced and robust Luxembourg DLT legal framework.

The Luxembourg House of Financial Technology (LHoFT) is a public-private initiative driving technological innovation for Luxembourg's financial service industry. It acts as an incubator for fintech initiatives and acts as a hub for the fintech ecosystem in Luxembourg. The LHoFT also offers additional support by connecting fintech initiatives with local service providers, investors, the University of Luxembourg and other associations.

A fintech company can also take advantage of the Luxembourg government's wider initiatives to help start-ups.

The Luxembourg legislator has decided not to create a regulatory sandbox for fintech start-ups, believing that it is important for new initiatives to incorporate regulatory requirements into the design phase of a product. The absence of a sandbox also gives start-ups greater credibility as it shows that they are mature enough to comply with comprehensive regulatory requirements.

Read this article on Lexology

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

In Luxembourg, the main regulator in charge of supervising fintech products and services is the Luxembourg Financial Sector Regulator (CSSF), which is the main regulator of the financial sector. Where insurance products are involved, this falls within the remit of the supervision of the Commissariat aux Assurances (CAA).

Alongside these regulators, are the Ministry of Finance and the Ministry of Justice, which are in charge of the development and implementation of new laws and initiatives in the fintech space.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Depending on the nature and scope of services, licensing requirements may be triggered in Luxembourg under the law of 5 April 1993 on the financial sector (the Financial Sector Law) and the law of 10 November 2009 on payment services (the Payment Services Law). The following activities are regulated activities as a matter of Luxembourg law:

- acceptance of deposits and other repayable funds;
- lending, including, inter alia, consumer credit, mortgage credit, factoring, with or without recourse, financing of commercial transactions;
- financial leasing;
- payment services as described in Annex I of Directive 2015/2366/EU (Payment Services Directive II) (PSD2), which has been replicated in Payment Services Law;
- Issuing and administering other means of payment (eg, travellers' cheques and bankers' drafts) insofar as this activity does not constitute payment services under PSD2;
- guarantees and commitments; and
- trading for own account or account of customers in:
    - money-market instruments (cheques, bills, certificates of deposit, etc);
    - foreign exchange;
    - financial futures and options;
    - exchange and interest-rate instruments; and
    - transferable securities; and
- participation in securities issues and the provision of services related to such issues;
- advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertakings;
- money broking;
- portfolio management and advice;
- safekeeping and administration of securities;
- credit reference services;
- safe-custody services;

Read this article on Lexology

- issuance of electronic money; and
- investment services in the sense of Directive 2014/65/EU (Markets in Financial instruments Directive II) (MiFID 2), including:

    - reception and transmission of orders in relation to one or more financial instruments;
    - execution of orders on behalf of clients;
    - dealing on own account;
    - portfolio management;
    - investment advice;
    - underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis; and
    - operation of an MTF.

Luxembourg has introduced a specific national equivalence regime with respect to investment services and activities whereby the CSSF has recognised a number of jurisdictions as 'equivalent'. This means that third-country firms (namely, a firm or a credit institution with its head office outside of the European Union) can under certain circumstances provide investment services or activities to professional clients or eligible counterparties (as defined in MiFID 2) in Luxembourg without having to establish a branch or obtain any other authorisation from the CSSF. An application form needs to be completed and submitted to the CSSF and the procedure is described in more detail in CSSF Circular 19/716 (as amended).

Currently, the following jurisdictions are deemed 'equivalent' by the CSSF: Australia, Canada, China, Hong Kong, Japan, Singapore, Switzerland, the United Kingdom and the United States according to CSSF Regulation 20/02 dated 29 June 2020, as amended from time to time.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Consumer lending is regulated in Luxembourg and requires a licence. Consumers are protected by the provisions of the Consumer Code.

For consumer lending, a number of formalities, such as the mandatory provision of information, have to be accomplished before a loan can be issued to a consumer.

Lending as a credit institution is also regulated in Luxembourg although certain exemptions apply:

- loans not made 'to the public'. The CSSF has clarified that this is where loans are granted:

    - to a limited circle of previously determined persons; or
    - the nominal value of a loan amount to €3 million at least (or the equivalent amount in another currency) and the loans are granted exclusively to professionals (as defined in the Consumer Code); and

- a lending activity that does not have a professional character, meaning that unique or one-off credit operations do not fall within scope; and

- loans between €200 and €75,000 do not fall within the scope of the Consumer Code.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

The trading of fully drawn loans does generally not trigger any licensing requirements in Luxembourg. There may be restrictions as well as licensing requirements for the trading of undrawn or partially drawn loans where the acquirer becomes the lender of record.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Undertakings for collective investments (UCIs) are governed by the law of 17 December 2010 and can take various legal forms. In general, to qualify as a UCI and fall within the scope of the legislation there needs to be a raising or injection of capital coupled with the issuance of units and a management of assets according to the principle of risk-spreading. Alternative finance products such as peer-to-peer lending may fall within the scope of this legal framework depending on the nature of the business. Where the fintech company manages assets on a pooled basis on behalf of investors, this legislation will need to be carefully considered. Additionally, fintech companies whose business involves managing one or more alternative investment funds (AIF) would need to consider the potential implications of Directive 2011/61/EU (Alternative Investment Fund Managers Directive) and the implementing Luxembourg law of 12 July 2013. An AIF is defined as a collective investment vehicle that raises capital from a number of investors, with a view to investing it in accordance with a defined investment policy for the benefit of those investors.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Alternative investment fund managers are regulated in Luxembourg and require a licence from the competent authority pursuant to the Luxembourg law of 12 July 2013 on alternative investment fund managers.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

There is currently no specific legal framework for peer-to-peer or marketplace lending in Luxembourg. Nevertheless, these activities could fall within the scope of the law of 5 April 1993 on the financial sector.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

Regulation (EU) 2020/1503 on European crowdfunding service providers for business is directly applicable in Luxembourg since 10 November 2021 and implies specific licensing requirements in Luxembourg.

The Regulation applies to crowdfunding services provided to project owners that are not consumers or crowdfunding offers with a consideration of more than €5 million per annum per project owner. The Regulation creates the new legal status of European crowdfunding service provider, benefiting from an EU passport after obtaining a licence in one member state. Licensing and supervision are carried out by the CSSF in Luxembourg.

Investor protection measures are also included in the Regulation, including mandatory information disclosures for project owners in the form of a key investment information sheet.

Crowdfunding service providers that also wish to provide payment services will need to obtain a separate licence.

According to Commission Delegated Regulation (EU) 2022/1988 of 12 July 2022, the transitional period (namely, according to which existing crowdfunding service providers, operating under national law, may continue to provide services within the meaning of the Regulation) is extended until 10 November 2023.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

Factoring operations consisting in the acquisition of commercial debts and in its recovery for own account is regulated by the law of 5 April 1993 on the financial sector and is considered as a lending operation. However, factoring operations that do not have credit elements are considered to fall outside of scope.

Payment services

12 | Are payment services regulated in your jurisdiction?

Yes, payment institutions are governed by the law of 10 November 2009 on payment services, which transposed PSD2. No person established in Luxembourg may provide payment services without holding a written authorisation from the CSSF. The regulated payment services follow those listed in Annex I of PSD2 and include:

- services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account;
- services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account;
- execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider:

  - execution of direct debits, including one-off direct debits;
  - execution of payment transactions through a payment card or a similar device; and
  - execution of credit transfers, including standing orders; and

- execution of payment transactions where the funds are covered by a credit line for a payment service user:

  - execution of direct debits, including one-off direct debits;
  - execution of payment transactions through a payment card or a similar device; and
  - execution of credit transfers, including standing orders; and

- issuing of payment instruments and (or) acquiring of payment transactions;
- money remittance;
- payment initiation services (namely, a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider); and
- account information services (namely, an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider).

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

Yes, in Luxembourg account information service providers are governed by the law of 10 November 2009 on payment services. This activity is characterised as an online service consisting of providing consolidated information regarding one or more payment accounts held by the user of payment services either with another payment service provider or with more than one payment service provider and is a regulated activity requiring a licence from the CSSF. Such service enables customers to access the information by online login on the account information service provider website. Like in the rest of the European Union, the drive for open banking was driven by PSD2 to optimise the customer's experience and increase competition and product innovation.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Robo-advisers that provide investment advice or execute orders have to be registered with the CSSF in the same manner as traditional providers of investment services. The exact type of licensing required depends on the services provided by the robo-adviser. There is currently no dedicated legal framework on automated advice for retail customers.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Yes, selling or marketing insurance products is regulated by the CAA and is governed by the law of 7 December 2015 on the insurance sector. In terms of insurance intermediation, Luxembourg regulations distinguish several categories such as agents, brokers and insurance intermediaries. Insurance intermediaries are subject to strict regulatory requirements, including having to evidence to the CAA their professional knowledge and experience. Depending on the type of product, Regulation (EU) No. 1286/2014 on packaged retail and insurance-based investment products may also be relevant.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Should a credit information service qualify as a credit-rating agency, Regulation (EC) No. 1060/2009 on credit rating agencies applies. Under this Regulation, a credit rating agency has to be registered if it is established in an EU member state.

Agencies have to adopt measures to prevent conflicts of interest and ensure that its credit ratings are based on a thorough methodological analysis of information.

There are currently no rules on providing consumer credit scores in Luxembourg.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

Credit institutions and investment firms authorised in an EU member state under one of the EU Single Market's Directives may be able to benefit from EU passporting and provide certain regulated activities in Luxembourg, either by way of freedom to provide services or by establishing a branch. Other EU financial institutions may also be able to benefit from EU passporting on the condition that they meet certain requirements, in particular, that it is a subsidiary of a credit institution. These regulated activities cover in particular those of credit institutions, Directive 2014/65/EU (Markets in Financial instruments Directive II) (MiFID 2) investment services and activities as well as the activities of payment service providers and electronic money institutions.

Firms will be able to passport and provide only those activities for which they are authorised in their home member state and there is a regulatory process with the home member state that needs to be followed.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

To obtain a licence for the services or activities regulated pursuant to the financial sector law or the law on payment services, a local presence is a prerequisite. Certain services can still be provided in or into Luxembourg, either under EU passporting or on a cross-border basis from a third country provided that certain criteria are respected and depending on the type of clients.

In accordance with Circular CSSF 20/743, fintech companies can rely on the reverse enquiry to avoid the licensing requirements when providing MiFID 2 services.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Depending on the regulatory status of the entities, different sales and marketing rules may apply. The consumer law framework contains provisions on information requirements, advertising and unfair contract terms. Consumer protection includes requirements to act fairly and honestly and to not mislead the customer and abide by minimum standards of market behaviour when dealing with consumers as well as general restrictions on the recording of telephone conversations, electronic commercial communications, conclusion of contracts by electronic means and doorstep selling.

Marketing materials for credit offerings must refer to the expected cost of the credit for the consumer and contain specific information depending on the type of credit and the purpose of the loan.

Marketing materials for investment services and complex products include all provisions related to European rules (eg, Directive 2014/65/EU (Markets in Financial instruments Directive II) and the Packaged retail investment and insurance-based products). The identification of marketing communications should be prominent and should include the appropriate disclaimer. Excessive cross-references to legal or regulatory provisions should be avoided unless this is appropriate. The suitability of the marketing communication must be considered taking into account the target retail investors and firms should avoid using technical wording. The information must be up-to-date, proportionate and sufficient for the customer to understand the key elements.

Where the products are funds, additional restrictions apply to the sale and marketing thereof.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

Luxembourg has implemented a law to allow for the possibility of using secure electronic recording systems, including Distributed Ledger Technology (DLT), for dematerialised securities.

In January 2022, the Luxembourg Financial Sector Regulator (CSSF) published a white paper on DLT and blockchain focusing on the risks and recommendations for the financial sector acknowledging that innovative processes and technologies can contribute to the improvement of the provision of financial services.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

The CSSF has adopted a tech-neutral approach, which means that it tries to regulate the output and risks of a system rather than the technology that a system is based on. Therefore, while there are no specific rules on cryptoassets, entities have to abide by the regulations that apply to traditional service providers in the same sector.

From a Luxembourg regulatory framework perspective, there is a specific regime for virtual asset service providers, which are rules with an anti-money laundering angle and in 2021, the CSSF also published its guidance on virtual assets along with two frequently asked questions for undertakings for collective investments and credit institutions.

The CSSF has issued several warnings advising retail clients against investing in this type of asset flagging that there are significant risks associated with them.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

There are currently no specific regulations in place for ICOs, but some general laws, such as the rules around the publication of a prospectus may apply to the issuance of tokens. The CSSF has published guidance and communication for consumers in the context of virtual assets including tokens.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

There is no specific regulatory framework for the use of artificial intelligence (AI). The Luxembourg Financial Sector Regulator (CSSF) has, however, adopted a soft-law instrument in the form of a white paper to help actors navigate the challenges of AI. Some forms of artificial intelligence utilising personal data are partially regulated by Regulation (EU) 2016/679 (General Data Protection Regulation). As the CSSF has adopted a tech-neutral approach, there is no legal distinction between robo-advice and traditional investment advice in Luxembourg and robo-advisers are therefore subject to the same licensing requirements as traditional investment advisers. On 3 May 2023, the CSSF, jointly with the Banque Centrale du Luxembourg, published a thematic review on the use of artificial intelligence in the Luxembourg financial sector.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

If an investor intends to acquire or increase a qualifying holding in a regulated company, this acquisition has to be notified to the Luxembourg Financial Sector Regulator (CSSF) and is subject to approval by the CSSF.

A qualifying holding is defined as any direct or indirect holding that represents 10 per cent or more of the capital, the voting rights (or both) or that makes it possible to exercise a significant influence over the management of the entity. Additionally, there are thresholds at 20, 33.3, 50 and 100 per cent that trigger a notification requirement if an existing shareholder increases (or decreases) its stake in a regulated entity. Where the entity is a credit institution the prior approval of the European Central Bank is required.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

There is no specific framework under which fintech companies are required to put in place procedures to combat bribery and money laundering. However, Luxembourg has introduced a specific regime of virtual asset service providers (VASPs). Luxembourg has implemented the Financial Action Task Force guidelines for 'virtual asset service providers' to register

with the Luxembourg Financial Sector Regulator (CSSF) for anti-money laundering (AML) and combatting financing terrorism purposes if they provide one or more of the following services on behalf of their clients or for their own account:

- exchange between virtual assets and fiat currencies, including the exchange between virtual currencies and fiat currencies;
- exchange between one or more forms of virtual assets;
- transfer of virtual assets;
- safekeeping or administration, or both, of virtual assets or instruments enabling control over virtual assets, including custodian wallet services; or
- participation in and provision of financial services related to an issuer's offer or sale of virtual assets, or both.

Virtual assets are defined as a digital representation of value, including a virtual currency, that can be digitally traded, or transferred, and can be used for payment or investment purposes and excludes financial instruments (as defined by Directive 2014/65/EU (Markets in Financial instruments Directive II)) and electronic money (as defined by Directive 2015/2366/EU (Payment Services Directive II)).

Therefore, these fintech companies are regulated by the CSSF, fall within the scope of the consolidated Luxembourg AML Law of 2004 and are required to implement the appropriate internal procedures and policies.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

Yes, with the VASP regime, the CSSF has published dedicated guidance with the aim of providing professionals with concise answers to the main practical issues they are facing. The CSSF has published guidelines in the form of a white paper aimed at helping interested professionals in the conduct of their due diligence process related to distributed ledger technology and its use in the provision of services in the Luxembourg financial sector. Finally, the Association of Luxembourg Banks and Bankers has developed AML solutions and services for fintech players.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

There are no legal requirements or regulatory guidance relating to personal data specifically aimed at fintech companies. The processing and transfer of personal data relating to fintech products and services are governed by Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR). The GDPR requires that controllers (the natural or legal person that determines the purpose and means of the processing of personal data) may

only process personal data where that processing is done in a lawful, fair and transparent manner, as further described in the GDPR. In particular, the processing of personal data must be done pursuant to one of six lawful bases for processing. The GDPR also places a significant burden on business, including, for example, mandatory requirements to notify regulators of data breaches, obligations to keep detailed records on processing and requirements for most entities to appoint a data protection officer.

GDPR rules only apply to information concerning an identified or identifiable natural person and do not apply to data that has been truly anonymised. Recital 26 gives limited guidance to determine whether a natural person is identifiable, requiring data controllers to take into account a number of factors, including the costs and time required to de-anonymisation taking into consideration the available technology at the time of the processing and technological developments.

When it comes to international data transfer, the GDPR sets up the rules to ensure that the level of protection of natural persons is not undermined by the fact that personal data are transferred to a third country. These rules aim to ensure that the country to which data is to be transferred provides a reasonable level of data protection.

In summary, a three-step test shall be carried out. First, the transfer shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed. Second, control of the basis of a tool on which the transfer relies shall be performed. Among the tools listed under Chapter V of the GDPR, the transfer may rely on an adequacy decision, issued by the European Commission, deciding that a third country ensures an adequate level of data protection. In the absence of a decision of adequacy, the transfer shall rely on one of the transfer tools listed under article 46 of the GDPR, such as the use of one of the model contracts approved by the European Commission (standard contractual clauses), binding corporate rules, codes of conduct, certification mechanism. Third, following the Court of Justice of the European Union *Schrems II* judgment (CJEU, 16 July 2020, Case C-311/18), issued in the context of the transfer of personal data to the United States, an additional step shall consist in assessing, on a case-by-case basis, if the legislation of the third country offers an adequate level of protection, taking into account the possible access to the personal data by public authorities. If the level of protection in the third country is not adequate, the adoption of supplementary measures is necessary to bring the level of protection of the data transferred up to the EU standard or essential equivalence. The European Data Protection Board issued recommendations containing concrete examples of supplementary measures.

Finally, a transfer to a third country or an international organisation can, in 'specific situations' take place on the grounds of the derogations set out in article 49 of the GDPR.

In Luxembourg, the law of 1 August 2018 contains additional provisions, and notably provides for the establishment of the National Commission for Data Protection, the Luxembourg Data Protection Authority, in charge of controlling compliance with the GDPR by businesses.

Read this article on Lexology

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

As of 18 October 2024, Directive 2016/1148/EU (Network and Information Systems) (NIS) will be repealed by Directive 2022/2555/EU (NIS2), dated 14 December 2022, which shall be implemented by the member states by 17 October 2024. Entities of the banking and financial sector fall within the scope of application of the NIS2 Directive. However, with regard to financial entities, this Directive shall be read in conjunction with Regulation 2022/2554/EU on digital operational resilience for the financial sector (DORA), which will be applicable as of 17 January 2025, with a direct effect in all member states.

DORA aims to consolidate all provisions addressing digital risk in the financial sector in one single act. The Regulation introduces more stringent requirements on information and communications technology (ICT) risk management and ICT-related incident reporting, including mandatory contractual provisions to be included in the contracts with ICT third-party providers.

Directive 2015/2366/EU (Payment Services Directive II) (PSD2), provides for, among others, rules concerning strict security requirements for electronic payments and the protection of consumer's financial data, guaranteeing safe authentication and reducing the risk of fraud. Luxembourg implemented the provisions of PSD2 by way of the law of 20 July 2018.

Further, the GDPR includes a few provisions relating to the security of the processing of personal data.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Yes, the Luxembourg Financial Sector Regulator (CSSF) Circular 22/806 on outsourcing arrangements consolidates the supervisory requirements for outsourcing by financial services companies. The CSSF complements the European Banking Authority Guidelines on the topic with detailed requirements applicable in Luxembourg and extends the scope of application to a wider range of financial institutions:

- credit institutions and their branches;
- investment firms and their branches;
- payment institutions and electronic money institutions and their branches; and
- other professionals in the financial sector and their branches.

This Circular describes internal governance requirements for planning, implementing, monitoring and managing outsourced activities and imposes requirements relating to

governance, risk management, conflicts of interest, internal controls, professional secrecy and business continuity.

The Circular also contains detailed requirements on ITC outsourcing the provisions of which also apply to other financial market players, including, for example, investment fund managers.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

Yes, CSSF Circular 22/806 specifies the regulatory framework for cloud computing infrastructure supplied by an external service provider. The CSSF considers that cloud computing is a form of outsourcing. The outsourcing to a cloud computing service provider by a regulated entity requires prior notification to the CSSF as well as internal governance and policies. The service contract between the financial institution and cloud computing service provider must, in principle, be subject to the laws of an EU member state and shall provide for the resiliency of cloud computing services. The regulated entity is also required to appoint a cloud officer who is responsible for the use of cloud services.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Computer programs (software) are protected by copyright (article 31 of the law of 18 April 2001 on copyright, related rights and databases). Copyright arises automatically as soon as the computer program is completed, provided that it is original. No further registration is required.

Databases underlying software programs may also be protected by copyright and, in certain circumstances, by database right (sui generis rights).

Software as well as business methods as such are expressly excluded from patentability. Software-implemented solutions may be protected by a patent if they show an 'additional technical effect'. The European Patent Office provides useful guidance in this respect.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

As a general principle, any assignment of copyright shall be made in writing (article 12 of the law of 18 April 2001). This requirement applies to intellectual property developed by

contractors or consultants. As a consequence, the author of the software owns the rights unless the contract provides for the contrary. The same goes for other intellectual property rights developed by a contractor or consultant.

An exception, however, exists in the case where software is developed by an employee during the course of their employment or pursuant to the employer's instructions. In this case, in the absence of a contractual agreement stating the contrary, the employer is exclusively entitled to exercise all economic rights on the software (article 32 of the law of 18 April 2001). The same goes for other intellectual property rights such as designs (article 3.29 of the Benelux Convention on intellectual property rights) or patents (article 13 of the law of 20 July 1992 amending the patent's legal framework).

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

An agreement is generally required between the joint owners of copyrights regarding their respective rights. In the absence of agreement, the rights must be exercised jointly.

However, unless otherwise provided by contract, each owner whose contribution to the work can be individualised, is entitled to individually exercise their rights, provided that:

- the exploitation is separate from the other joint owners' exploitation; and
- this individual exploitation will not harm the work (article 5 of the law of 18 April 2001).

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Trade secrets are protected by the law of 26 June 2019 on the protection of undisclosed know-how and business information (implementing Directive 2016/943/EU (Protection of Trade Secrets). This law defines trade secrets as information that:

- is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- has commercial value because it is secret; and
- has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Trade secrets may be kept confidential during court proceedings relating to the unlawful obtaining, use or disclosure of a trade secret, under the conditions set out in article 14 of the law of 26 June 2019. The protection may be granted ex officio by the judge or at the request of a disputing party.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brands can be protected by a Benelux trademark (covering Belgium, the Netherlands and Luxembourg) or by EU trademark (covering EU territory). A Benelux trademark shall be registered with the Benelux Office for Intellectual Property (BOIP), and the EU trademark shall be registered with the European Union Intellectual Property Office (EUIPO). Both BOIP and EUIPO hold public databases where it is possible to control the availability of a trademark.

A preliminary search in the Luxembourg Business Register and on the internet is also advised to check the availability of any trade or company name.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

In the case of infringement, interim measures (such as immediate cessation of the breach and seizure of goods) can be ordered by a court on the basis of the law of 22 May 2009 on the enforcement of intellectual property rights. Damages can also be claimed pursuant to the Benelux Convention for intellectual property.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

General competition law applies to fintech companies (law of 23 October 2011 regarding competition, prohibiting anticompetitive agreements and the abuse of dominance) as well as EU competition rules. On 24 November 2022, the Chamber of Deputies adopted draft law 7479A on competition, which aims to transpose Directive 2019/1/EU (European Competition Network Plus) (ECN+). With the entry into force of the law, the Competition Council, an independent administrative authority, is transformed into a public establishment now called the Competition Authority of the Grand Duchy of Luxembourg, notably to meet the independence requirements imposed by ECN+.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

Luxembourg did not introduce, as such, specific tax incentives for fintech companies only. This can be explained by the fact that Luxembourg already offers a very favourable tax framework for the development of the financial sector.

Luxembourg benefits from one of the lowest value added tax rates within the European Union (16 per cent for 2023) and moderated corporate income tax rate (namely, an overall rate of 24.94 per cent including municipal business tax and solidarity surcharge). One of the huge strengths of the country resides in its extended network of double tax treaties which guarantees the absence of situations of double taxation, for instance on cash repatriation mechanisms.

Luxembourg also offers an attractive environment for intellectual property investments with an 80 per cent exemption from corporate tax on income and gains derived from eligible rights. In addition, there is no withholding tax on royalty and assimilated payments made by a Luxembourg capital company.

Luxembourg entities involved more specifically in innovative research and development activities can benefit from financial support in addition to the specific intellectual property regime.

On top of these advantages, formation expenses of start-ups can be subject to depreciation. Certain investments can benefit from a tax credit of up to 13 per cent (for investments in tangible depreciable assets).

Finally, Luxembourg is an attractive country for new talents. With the specific tax regime applicable to inpatriates, foreign talents coming to Luxembourg may, subject to certain conditions, benefit from a tax exemption for certain costs borne by their employer and from certain benefits granted by the latter in the context of the relocation of the employee to Luxembourg. It applies during a period of several years.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

To date, the Luxembourg tax framework is not extensive with respect to the regulation of the fintech sector. There are, for instance, no specific tax laws regulating cryptocurrencies or cryptoassets. The only relevant regulation is the administrative circular issued by Luxembourg tax authorities back in 2018, where they stated in summary that cryptocurrencies were not to be considered functional currencies for tax purposes and that the taxpayer should qualify the cryptoasset according to general tax principles and apply the related tax treatment to the income derived from said asset.

Read this article on Lexology

However, the fintech sector has significantly evolved since 2018 and more specific guidelines would be welcomed. Regulation is not always synonymous with administrative burden or increase of costs and we believe that such an effort from the legislator could help even further in the development of the fintech sector.

Financial intermediaries of the fintech sector are not, for the time being, concerned by the obligations related to the exchange of information between EU tax authorities. However, with the proposed extension of Council Directive 2011/16/EU (Directive on Administrative Cooperation VIII) (DAC8), it is expected that reporting obligations and subsequent obligations of exchange of information would be imposed on cryptoasset service providers and issuers. The introduction of DAC8 is still at the very beginning of the EU legislative process but there is no doubt that this new set of obligations would go ahead and become a reality for all concerned EU taxpayers.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

There are no fintech-specific immigration schemes in Luxembourg. The usual regime will apply and will depend on the nationality and residence of the staff that the Luxembourg entity would wish to employ. Visa requirements may be applicable.

UPDATE AND TRENDS

Current developments

41 Are there any other current developments or emerging trends to note?

Luxembourg has an innovative local fintech start-up scene, which is developing digital tools to help companies and financial institutions.

The adoption of the EU Markets in Crypto-assets Regulation at the EU level on 20 April 2023 is a game-changer for the fintech space. The Regulation proposes harmonisation of the requirements across the European Union and authorised service providers are now able to benefit from EU passporting to provide regulated services on a cross-border basis, as we know for many other regulated financial services.

Cathrine Foldberg Møller	cathrine.foldberg-moller@simmons-simmons.com
Julie Carbiener	julie.carbiener@simmons-simmons.com
Camille Saettel	camille.saettel@simmons-simmons.com
Camille Bénézet	camille.benezet@simmons-simmons.com
Maya Coumes	maya.coumes@simmons-simmons.com

Royal Monterey, 26A Boulevard Royal, Luxembourg 2449, Luxembourg
Tel: +352 26 21 16 01
www.simmons-simmons.com

Read more from this firm on Lexology

Read this article on Lexology

Malta

Leonard Bonello and James Debono
Ganado Advocates

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 371
General innovation climate 371
Government and regulatory support 372

FINANCIAL REGULATION 372
Regulatory bodies 372
Regulated activities 373
Consumer lending 373
Secondary market loan trading 374
Collective investment schemes 374
Alternative investment funds 375
Peer-to-peer and marketplace lending 375
Crowdfunding 375
Invoice trading 376
Payment services 376
Open banking 376
Robo-advice 376
Insurance products 377
Credit references 377

CROSS-BORDER REGULATION 378
Passporting 378
Requirement for a local presence 378

SALES AND MARKETING 378
Restrictions 378

CRYPTOASSETS AND TOKENS 379
Distributed ledger technology 379
Cryptoassets 379
Token issuance 380

ARTIFICIAL INTELLIGENCE 380
Artificial intelligence 380

CHANGE OF CONTROL 380
Notification and consent 380

Read this article on Lexology

FINANCIAL CRIME 381
Anti-bribery and anti-money laundering procedures 381
Guidance 382

DATA PROTECTION AND CYBERSECURITY 382
Data protection 382
Cybersecurity 382

OUTSOURCING AND CLOUD COMPUTING 383
Outsourcing 383
Cloud computing 383

INTELLECTUAL PROPERTY RIGHTS 384
IP protection for software 384
IP developed by employees and contractors 384
Joint ownership 385
Trade secrets 385
Branding 386
Remedies for infringement of IP 386

COMPETITION 387
Sector-specific issues 387

TAX 387
Incentives 387
Increased tax burden 387

IMMIGRATION 388
Sector-specific schemes 388

UPDATE AND TRENDS 388
Current developments 388

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Malta's reputation as the 'blockchain island' is a testament to its positive approach to the fintech industry. Malta was a pioneer in regulating distributed ledger technologies and cryptocurrencies through the enactment of:

- the Virtual Financial Assets Act, Chapter 590 of the Laws of Malta;
- the Malta Digital Innovation Authority Act, Chapter 591 of the Laws of Malta (MDIAA); and
- the Innovative Technology Arrangements and Services Act, Chapter 592 of the Laws of Malta.

Other prominent fintech areas attracting investment in Malta relate to e-payment services and insurtech. Further, the Malta Financial Services Authority (MFSA) buttressed this technological revolution by setting up the dedicated FinTech and Innovation function. The MFSA

Read this article on Lexology

is also driving the long-term fintech strategy targeting both start-ups and industry scale-ups with the aim of establishing Malta as an international fintech hub while promoting the infusion of technology solutions in the financial world.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

The Maltese government has always given the fintech industry priority in policy formation. The MFSA has launched the standalone FinTech Strategy aimed at providing legal and regulatory certainty and ensuring market integrity and financial soundness while safeguarding investor rights in the fintech sphere. This strategy is based on six main pillars, namely:

- a suite of regulations to support regulatory efficiency;
- a holistic all-encompassing ecosystem to enhance access to finance and foster innovation;
- implementing an open architecture to support the use of application programming interfaces in financial services;
- fostering international links to enhance bilateral cooperation and cross-border fintech knowledge, adoption and investment;
- cultivating knowledge by attracting and retaining talent and carrying out extensive research; and
- security through implementing robust systems, plans and techniques to counteract threats and exposure.

The strategy also features a regulatory sandbox that enables financial service providers to test the viability of their products within the regulatory framework, while keeping in direct contact with the regulators.

The Malta Digital Innovation Authority (MDIA) is a relatively new regulator that was established to act as:

- a fintech promoter that incentivises 'investment' in 'innovative technology arrangements', as such terms are defined under the MDIAA; and
- a supervisory authority that ensures the reliability of these technologies and the integrity of the market.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

The Malta Financial Services Authority (MFSA) and the Malta Digital Innovation Authority are the main competent authorities regulating the provision of fintech products and services.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

The local financial services regulatory framework comprises:

- the Investment Services Act, Chapter 370 of the Laws of Malta (ISA), which outlines the regulatory requirements of operators wishing to set up investment services undertakings and collective investment schemes. It transposes the Markets in Financial Instruments Directive II (2014/65/EU) (MiFID 2) into Maltese law and regulates services outlined therein when they are carried out in or from Malta and in relation to one or more 'instruments', as defined therein;
- the Banking Act, Chapter 371 of the Laws of Malta, which is the law regulating credit institutions that carry out the 'business of banking', defined as:
    - accepting deposits of money from the public that are withdrawable or repayable on demand, after a fixed period or after notice;
    - borrowing or raising money from the public with the purpose of using all or some of such money to lend to others; or
    - otherwise investing for the account and at the risk of the person accepting this money; and
- the Financial Institutions Act, Chapter 376 of the Laws of Malta (FIA), which sets out the licensing and ongoing obligations of non-banking institutions. These can be classified into two categories; namely, institutions that carry out:
    - payment services or the issuance of electronic money; and
    - activities such as lending, financial leasing, the provision of guarantees and commitments, foreign exchange services and money brokering.

The FIA, the subsidiary legislation and the regulations promulgated under the FIA transpose the second Payment Services Directive (2015/2366/EU) (PSD2) and the second Electronic Money Directive (2009/110/EC), are:

- the Virtual Financial Assets Act, Chapter 590 of the Laws of Malta (VFAA), which regulates services that are provided in relation to distributed ledger technology assets that have been determined to be a virtual financial asset. Such services listed in the VFAA are mostly similar to those listed in the ISA; and
- the Insurance Business Act, Chapter 403 of the Laws of Malta (IBA), which regulates the business of insurance, namely, effecting and carrying out contracts of insurance for long-term business or general business as defined in the IBA.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Lending is a regulated activity under the Banking Act as it falls under the definition of 'business of banking', which requires a licence in Malta. Moreover, lending is a regulated activity under the FIA, irrespective of whether it is provided to consumers. Article 5 of the

FIA outlines the requirements for the authorisation of an institution to carry out lending activities, including:

- an initial capital in the amount established by the MFSA;
- at least two individuals effectively directing the business of the institution in Malta;
- all qualifying shareholders, controllers and all persons effectively directing the institution's business are suitable persons to ensure its prudent management; and
- sound and prudent management and robust governance arrangements.

In addition:

- the Consumer Credit Regulations (Subsidiary Legislation 378.12) implement into Maltese law the provisions of the Consumer Credit Directive (Directive 2008/48/EC), which regulates credit agreements involving a total amount of credit more than €200 or less than €75,000, which are provided to consumers; and
- the Credit Agreements for Consumers relating to Residential Immovable Property Regulations (Subsidiary Legislation 378.10) of the laws of Malta, which implement into Maltese law the provisions of the Mortgage Credit Directive (Directive 2014/17/EU).

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

There are no particular restrictions applicable to trading loans in the secondary market in Malta.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Collective investment schemes (CIS) are regulated under the ISA. CIS that fall within the scope of the local regulations are:

- retail collective investment schemes, primarily undertaking collective investment transferable securities;
- professional investor funds;
- alternative investment funds (AIFs); and
- notified alternative investment funds.

Investment-based crowdfunding is regulated under a separate regime.

With respect to peer-to-peer (P2P) or marketplace lenders, it is pertinent to refer to the FIA, which regulates 'money broking', defined as the activity of introducing counterparties that wish to deal at mutually agreed terms with respect to wholesale and retail financial products. This regulation may have implications for both marketplace lenders and P2P platforms.

Read this article on Lexology

Alternative investment funds

8 Are managers of alternative investment funds regulated?

An alternative investment fund manager (AIFM) who operates in or from Malta fall within the scope of the ISA and the Alternative Investment Fund Managers Regulations (Subsidiary Legislation 370.23 of the Laws of Malta), which transpose the Alternative Investment Fund Managers Directive (2011/61/EU) (AIFMD) into Maltese law. An AIFM may be subject to a lite regime akin to the regime under MiFID 2 if it qualifies as a de minimis AIFM. This will be the case where the assets under management are worth less than:

- €100 million; or
- €500 million and the portfolio consists of AIFs that are unleveraged and have no redemption rights in the first five years following the date of initial investment.

A de minimis AIFM will be exempt from complying with certain provisions of the AIFMD but does not enjoy the use of EU passporting rights.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

The FIA stipulates that any person that, as a lender, regularly lends money in or from Malta is carrying out a regulated activity and requires an MFSA licence prior to commencing operations. However, there is no specific regulation on P2P platforms or marketplace lending under the local financial services framework.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

While reward-based and donation-based crowdfunding platforms remain unregulated, the MFSA had introduced a framework initially under the ISA applicable to investment-based crowdfunding services and was now replaced by a completely separate licensing and regulatory framework specifically regulating crowdfunding platform service providers in light of Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 (ECSP Regulation).

The ECSP Regulation is directly applicable in Malta and requires entities providing crowdfunding services to be authorised by the competent authority. By virtue of the Malta Financial Services Authority Act (European Crowdfunding Service Providers for Business) Regulations (Subsidiary legislation 330.15) of the laws of Malta, the MFSA is the designated competent authority and has issued Crowdfunding Rules to which Crowdfunding Service Providers are subject.

The Parliament of Malta is currently discussing the Crowdfunding Service Providers Bill, which will mainly give effect to the provisions of Regulation (EU) 2020/1503 of the European

Read this article on Lexology

Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937. The same bill aims to inter alia establish a regulatory framework for crowdfunding services, particularly focusing on their organisation, authorisation and supervision of crowdfunding service providers, as well as for transparency and marketing communications in relation to the provision of crowdfunding services in the European Union.

Further, the European Securities and Markets Authority (ESMA) has published the draft technical standards on crowdfunding under Regulation (EU) 2020/1503.

Invoice trading

11 Describe any specific regulation of invoice trading in your jurisdiction.

Invoice trading falls within the scope of the FIA. Factoring and invoice discounting are listed as two types of lending activity that in turn trigger a licensing obligation under the FIA if and when they are carried out in or from Malta on a regular basis.

Payment services

12 Are payment services regulated in your jurisdiction?

The FIA includes a list of the payment services that are regulated in Malta and reflects the services outlined in the PSD2. Institutions engaging in these payment activities must obtain authorisation from the MFSA prior to the provision of these services in or from Malta on a regular basis.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

There are no laws or regulations promoting competition among financial institutions through the use of available data. However, the concept of open banking has been locally introduced under the Financial Institutions Act through the regulation of third-party payment service providers, namely, payment initiation service providers and account information service providers.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

No laws or regulations specific to robo-advisers or automated access to investment products have been issued in Malta.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Insurance and reinsurance undertakings carrying on the business of insurance in or from Malta including (re)insurance distribution activities or market (re)insurance services in or from Malta are regulated by two legislative instruments, namely:

- the Insurance Business Act, Chapter 403 of the Laws of Malta; and
- the Insurance Distribution Act, Chapter 487 of the Laws of Malta.

These Acts impose requirements from or with the MFSA depending on the nature of the insurance business activity being provided in or from Malta. These Acts, which implement EU Directive 2009/138/EC and EU Directive 2016/97/EU respectively, are supplemented by regulations promulgated under these two laws and by rules and guidelines issued by the MFSA.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

'Credit reference agency' is defined under the Trading Licence Act, Chapter 441 of the Laws of Malta and its subsidiary legislation, as any undertaking licensed by the Trade Licensing Unit, whose main business is to prepare, assemble and evaluate credit information and related credit and risk management services concerning legal and natural persons for the purpose of issuing credit scores to be furnished to third parties, provided that the agency is not precluded from carrying out other related tasks. The definition of 'credit reference agencies' pursuant to the draft law falls outside the scope of Regulation (EC) 1060/2009 and, therefore, ESMA would not have supervisory powers over these entities. Further, credit reference services are listed under the Banking Act as one of the additional activities exercisable by credit institutions.

The Central Bank of Malta Act, Chapter 204 of the Laws of Malta provides that credit reference agencies must be licensed by the Trade Licenses Unit in terms of regulation 47A of the Trading Licences Regulations, and the Central Bank of Malta is the supervisory authority in this regard solely for the purpose of overseeing and regulating the issuance of credit scores. The Central Bank has issued Central Bank of Malta Directive No. 15 on the Supervision of Credit Reference Agencies, which sets out the requirements to be met by licensed credit reference agencies.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

Regulated activities emanating from EU directives transposed into Maltese law can, subject to regulatory and procedural formalities, be passported into Malta. Credit and financial institutions, investment services providers, collective investment schemes and issuers that are legally established in one member state may passport their services through the establishment of a branch or otherwise, as may be applicable. Conversely, 'homegrown' services that are regulated by a standalone legislative framework in EU member states cannot be passported into Malta.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

Fintech companies cannot obtain a licence without establishing a local presence in Malta. While local presence and substance requirements vary across the different regulatory regimes applicable to the specific services being provided by a fintech company, a degree of substance in Malta is always required.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

The Malta Financial Services Authority (MFSA) has the discretional authority to issue marketing guidelines and restrictions that apply to various financial services sectors and to prohibit or alter any kind of promotional activity carried out by any financial services institution. Specific restrictions apply to licence holders that market their services and products to ensure that all information including marketing communications addressed to retail investors or potential retail investors is fair, clear and not misleading. The Investment Services Act states that no collective investment schemes, licensed or otherwise, can issue or cause to be issued a prospectus in or from Malta unless it has been approved by the MFSA. The marketing of retail financial services in Malta also falls within the scope of the Distance Selling (Retail Financial Services) Regulation (Subsidiary Legislation 330.07), which implements EU Directive 2002/65/EC.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

The Innovative Technology Arrangements and Services Act (ITAS) outlines the framework of designated innovative technology arrangements (including blockchain platforms and smart contracts) while catering for the Malta Digital Innovation Authority (MDIA) and its regulatory functions with regard thereto. Under the ITAS, any person may, on a voluntary basis, request the MDIA to certify eligible arrangements or services on the basis of a number of conditions, including that, among other things, the arrangement is fit and proper for the purposes for which it was set up and its underlying software has been reviewed by a registered systems auditor.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

Crypto-assets in Malta are regulated by the Virtual Financial Assets Act (VFAA), which spearheads the implementation of a bespoke financial instrument test, applicable to issuers, agents and licence holders, for the purpose of determining whether a distributed ledger technology (DLT) asset qualifies as:

- electronic money;
- a financial instrument;
- a virtual financial asset (VFA); or
- a virtual token.

If a person provides any of the services listed in the VFAA in relation to a DLT asset that qualifies as a VFA, licensing obligations apply. The issuance of e-money also mandates a Malta Financial Services Authority (MFSA) authorisation pursuant to the Financial Institutions Act.

In relation to NFTs, the MFSA has indirectly pronounced itself through a consultation document by saying that it considers that it would be prudent that certain VFAs, which display clear characteristics of uniqueness and non-fungibility, also be excluded from the VFA Framework, and therefore should remain unregulated (reflecting the approach taken under the Markets in Crypto-Assets Regulation.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

The VFAA imposes a licensing requirement on service providers in the VFA space, including VFA exchanges, custodians of VFAs (including wallet providers) and VFA advisers and brokers that are operating in or from Malta. The MFSA has issued a Virtual Financial Assets Rulebook, which is divided into three main chapters. The requirements for a VFA service provider licence include:

- the setting up of a Maltese entity;
- the holding of minimum capital; and
- the appointment of various functionaries and undergoing assessments by the MFSA into (among other things) the entity's ultimate beneficial owners and board of administration.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

Artificial intelligence (AI) is not yet a regulated area. A Malta AI task force, commissioned by the government launched the Strategy and Vision for Artificial Intelligence in Malta 2030, to put the island among the foremost jurisdictions with the highest-impact national AI programme. The strategy rests on three vertical pillars that direct efforts towards investment, innovation and private and public sector adoption; and three horizontal enablers, namely education and workforce, the legal framework and infrastructure.

In the meantime, the European Union issued its Proposal on Artificial Intelligence.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

The Investment Services Act imposes a notification requirement for persons who, directly or indirectly, acquire a 'qualifying shareholding' (as defined therein) in an investment services licence holder or increase their qualifying shareholding to an extent that the proportion of the voting rights or the capital held would reach or exceed 20 per cent, 30 per cent or 50 per cent or so that the investment services licence holder would become its subsidiary. The Malta Financial Services Authority (MFSA) can object to such an acquisition. A notification obligation is also triggered in the case of disposal or reduction of such qualifying

shareholding. Licence holders must obtain written consent from the MFSA before acquiring 10 per cent or more of the voting share capital of another company before agreeing to sell or merge all or any part of its undertaking.

In the context of credit institutions, Banking Rule 13/2021, 'Prudential assessment of acquisitions and increase of qualifying shareholdings in credit institutions authorised under the Banking Act', provides a blueprint of the procedural rules and evaluation criteria for the prudent assessment of acquisitions and holdings increases in the financial sector and determines the criteria to be applied by the MFSA in the assessment process of a proposed acquirer. These rules reflect the Joint Guidelines JC/GL/2016/01, which were issued by the Joint Committee of the European Supervisory Authorities in 2016, and also reflect the updated Appendix 1 in view of the publication of Standards (regulatory technical standards) under article 8(2) of Directive 2013/36/EU (EBA/RTS/2017/08).

Under the Financial Institutions Act, Chapter 376 of the Laws of Malta, changes to the qualifying shareholding of a financial institution licensed by the MFSA, also trigger an approval process akin to that applicable to credit institutions.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

The regulatory framework that governs anti-money laundering (AML) procedures in Malta falls under the Prevention of Money Laundering Act, Chapter 373 of the laws of Malta (PMLA) and the Prevention of Money Laundering and Funding of Terrorism Regulations, which implements EU Directive 2015/849/EU. The European Union extended the scope of its AML regime to digital currencies through EU Directive 2018/8432/EU. Entities that must abide by the AML regulations include those that:

- provide services to safeguard private cryptographic keys on behalf of its customers, or to hold, store and transfer virtual currencies; and
- engage in exchange services between virtual currencies and fiat currencies.

Malta has acknowledged the risks associated with digital currencies and has taken the initiative to anticipate this framework. The new Implementing Procedures issued by the Financial Intelligence Analysis Unit (FIAU) now also cover issuers of virtual financial assets (VFAs), VFA service providers and the activities of safe custody services, even when provided by any person or institution other than those licensed or authorised under the Banking Act or the Investment Services Act. Digital currency exchanges and issuers of VFAs are deemed to be subject persons and must have measures, policies and procedures in place to address the identified risks. These measures, policies, controls and procedures must include, inter alia:

- customer due diligence, record-keeping procedures and reporting procedures; and
- risk management measures.

Read this article on Lexology

The FIAU had also issued a consultation paper for the enactment of the Prevention of Money Laundering Act (Transfer of Virtual Financial Assets) Regulations to provide for the information that is to be transmitted simultaneously or concurrently with all transfers of virtual financial assets, in line with FATF Recommendation 16, referred to as the Travel Rule, which provides that virtual assets service providers that transmit digital funds should collect and exchange user information and make this available to relevant authorities if required.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

The FIAU has issued a specific rulebook applicable to VFA agents, issuers and licence holders with sector-specific guidance on how these issuers and operators can meet their AML obligations under the PMLA. These procedures complement the Implementing Procedures that are applicable across all other sectors, and apply to VFA service providers, VFA agents and issuers of initial VFA offerings, as well as to unlicensed subject persons operating within the VFA space.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

There is no specific law or guidance regulating fintech companies' use of personal data. The processing and transfer of data is regulated by the Data Protection Act, Chapter 586 of the Laws of Malta (DPA), which implements the EU General Data Protection Regulation (Regulation (EU) 2016/679), alongside any subsidiary legislation that supplements the DPA, and regulates the processing of personal data with regards to the e-communications sector, thereby implementing EU Directive 2002/58/EC.

The European Commission has issued draft proposals for an e-privacy regulation to supersede the current Directive (2002/58/EC), which would be directly applicable in all member states, harmonising data protection laws. On 21 February 2020, the revised text of the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) was published.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

Different cybersecurity standards apply across different business sectors within the financial industry. In the digital assets space, which is regulated by the Virtual Financial Assets Act, licence holders must establish various management policies within their cybersecurity

framework. Further, acknowledging that the financial services industry is experiencing a digital and technological transformation, the Malta Financial Services Authority has issued a new set of guidance notes on cybersecurity, which will apply to key players in this industry, setting out a minimum set of best practices and risk management procedures to be followed to effectively mitigate cyber risks.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

In general, the outsourcing of material services or activities of a financial services company would lead to the regulatory intervention and oversight of the Malta Financial Services Authority (MFSA). For example, the Banking Act provides that no credit institution shall outsource its material services or activities, unless the outsourcing service provider is granted recognition by the MFSA. To obtain this recognition, the outsourcing service provider must make a written request providing information on inter alia:

- its name and address;
- the material services or activities to be outsourced;
- the reasons for outsourcing the service or activities; and
- the regulatory status, if any, if it is authorised or licensed in a foreign jurisdiction.

The MFSA has issued Banking Rule 14 on Outsourcing by Credit Institutions Authorised under the Banking Act (which is applicable both to credit and financial institutions). The MFSA has also issued Guidance on Technology Arrangements, ICT and Security Management, and Outsourcing Arrangements that are applicable to all licence holders and set out the requirements for internal governance arrangements on ICT and security risk management as well as outsourcing requirements.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

Various initiatives at both a local and European level seek to govern the evolution of cloud computing. However, these are not necessarily specific to the financial services sector. Locally, the Malta Communications Authority has issued a guidance document titled 'Cloud Computing Guidelines for SMEs and Microenterprises' that highlights considerations to be taken by small and medium-sized enterprises and microenterprises when assessing the suitability of the use of cloud computing in their firm. This guidance document provides further details as to the contractual implications that may arise between small and medium-sized enterprises, microenterprises and cloud computing service providers. Transposing EU Directive 2016/1148/EU, Subsidiary Legislation 460.35 sets out cybersecurity standards and establishes a Critical Information Infrastructure Protection Unit (CIIP Unit). In Malta, the

CIIP Unit falls under the remit of the Critical Infrastructure Protection Directorate, which also oversees the National Computer Security Incidence Response Team.

The MFSA Guidance on Technology Arrangements, ICT and Security Management, and Outsourcing Arrangements sets out requirements in relation to the adoption of cloud computing resources and services and has also issued Guidance on Software-as-a-Service as an Outsourcing Arrangement, providing practical guidelines as to the approach to be adopted by licence holders in this regard. The European Securities and Markets Authority Guidelines on Outsourcing to Cloud Service Providers have been implemented in various MFSA Rulebooks.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Software constitutes literary work, which enjoys automatic copyright protection under the Copyright Act, Chapter 415 of the Laws of Malta. A copyright is a non-registrable right that arises as soon as a work considered eligible for copyright protection (which under Maltese law, includes artistic works, audiovisual works, databases, literary works and musical works) is created. No formal registration of copyright (voluntary or otherwise) in Malta is required. Further, in accordance with the Patents and Designs Act, Chapter 417 of the Laws of Malta (PDA), schemes, rules and methods for doing business and computer programs are not considered to constitute inventions that are capable of patent protection.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

In terms of works that are eligible for copyright protection, the Copyright Act dictates that such protection shall vest initially in the author or joint authors of the particular work. Particularly in the case of computer programs and databases, however, where a work is made in the course of the author's employment, the economic rights arising therefrom will be deemed to be transferred to the author's employer – subject to an agreement between the parties to the contrary. Other works eligible for copyright (namely, barring computer programs and databases) shall always vest in the author or joint authors of the particular work, provided that an agreement to the contrary has not been entered into.

With reference to patentable inventions, the PDA holds that any invention occurring under a contract of employment belongs to the employer; however, the creator of that work (namely, in this context, the employee) would have a right to equitable remuneration for their invention. In the absence of an agreement between the parties as to the remuneration due, this must be ascertained by the Maltese courts.

In view of the various nuances highlighted above, it is always advisable to incorporate a clause regulating the ownership, or otherwise, of intellectual property into a company's standard contract of employment and service agreements with its contractors or consultants. However, when developing or making use of intellectual property in the course of employment or engagement, there is an argument to be made that the employee or the contractor or consultant engaged to render a particular service must be considered a fiduciary in accordance with article 1124 et seq of the Civil Code Chapter 16 of the Laws of Malta and must therefore abide by the various obligations specified therein.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

The Trademarks Act, Chapter 597 of the Laws of Malta, states that where a registered trademark is subject to co-ownership, each joint owner is entitled, subject to an agreement stating the contrary, to an equal undivided share in the registered trademark. Each co-owner is also entitled, personally or otherwise, to perform for their own benefit, without the other co-owner's consent, any act that would otherwise amount to an infringement of the registered trademark. A co-owner may not grant a licence over the registered trademark or assign or cede control of their share in the trademark without the other co-owner's consent.

The aforementioned is also applicable in the case of co-ownership of a registered design under the PDA. Conversely, in the case of joint proprietors of a patent, the law specifies that either party may separately assign or transfer by succession their share of the patent with or without the other patent owner's agreement. However, to surrender the patent or conclude a licensing agreement with third parties, the co-owners must act jointly.

In terms of copyright, a joint author can assign or license copyright unilaterally, provided that where any other joint author is not satisfied with the manner in which this assignment or licence has been granted, they can resort to the Copyright Board within three months from the day on which the terms of the assignment or licence have been communicated to them in writing.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

The Trade Secrets Act, Chapter 589 of the Laws of Malta (TSA) provides for measures to be taken against the unlawful acquisition, use and disclosure of trade secrets. The TSA allows the competent court to issue precautionary acts against the alleged infringer for the cessation or prohibition of the use or disclosure of the trade secret on a provisional basis. The court may also issue precautionary acts to prohibit the production, offering, placing on the market or use of infringing goods or the seizure of these infringing goods to prevent their entry into or circulation on the market. Once the court has determined that there has been unlawful acquisition, use or disclosure of a trade secret, it can order the cessation of the unlawful behaviour, apply injunctive and corrective measures or impose damages that are appropriate to the actual prejudice suffered as a result of the unlawful acquisition, use or

disclosure of the trade secret. The TSA also states that should an application be submitted by an interested party, it shall be unlawful for any of the parties participating within the legal proceedings to disclose the nature or any details relating to the trade secret in question. This obligation shall remain in force even after legal proceedings have ended.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Trademarks create a distinctive brand and can be obtained by lodging an application with the Malta Intellectual Property Rights Directorate outlining the trademark name or image (or combination thereof), as well as the goods and services that this trademark will protect. It is also possible to apply for an EU trademark, which will grant pan-EU protection over the trademark. On an international level, it is also possible to lodge an application with the World Intellectual Property Organisation, designating the countries in which trademark protection is sought.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

The remedies available are enshrined in the acts that regulate specific IP rights. The Trademarks Act provides that a person found guilty of trademark infringement under this act may be liable for:

- imprisonment for up to three years;
- a fine of up to €23,293; or
- both.

This liability attaches to any person who, with a view to gain for themselves or another, or with intent to cause loss to another, uses or applies without the consent of the trademark owner an infringing sign or else has in their possession or control or offers for sale, hire or distribution goods that bear infringing marks. The Enforcement of Intellectual Property Rights (Regulation) Act, Chapter 488 of the Laws of Malta, provides for measures that may be requested by intellectual property rights holders to enforce their intellectual property rights or to preserve evidence and request information from alleged infringers.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

There are no competition issues that specifically affect fintech companies in Malta. However, in 2019, the European Commission published its Competition Policy for the Digital Era, which tackles competition issues that arise from the digital industries and states how regulations should be tailor-made to cater for the specific issues that might arise. The report identified the following characteristics of the industry that might give rise to incentives for dominant digital firms to act in an anticompetitive manner:

- the extreme returns to scale that the industry brings with it;
- the convenience of the product being dependent on a large user base; and
- the pivotal role of data.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

While the Maltese corporate tax environment is very attractive to businesses establishing a local presence, there do not seem to be tax incentives specifically available for fintech companies. Malta offers several fiscal schemes and incentives in the form of tax credits to companies deemed as being innovative enterprises according to the rules and regulations set out by Malta Enterprise.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

Without prejudice to the regulatory fees payable to the competent authorities in relation to any new licensing obligations imposed on fintech companies, there are no new or proposed tax laws or guidance specific to fintech businesses that will amplify tax and administrative costs.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

At present, in Malta, there are no immigration regimes specifically targeting fintech businesses aspiring to recruit skilled staff from abroad, which means that the immigration schemes that are available to fintech businesses are no different from the schemes that are available to other business sectors.

There are two regimes available, distinguishing EU, EEA and Swiss nationals from non-EU nationals. EU, EEA and Swiss nationals aspiring to work in Malta's fintech business must apply for residence via CEA Form A submitted on the basis of employment or self-employment pursuant to the Free Movement of EU Nationals and their Family Members Order (LN 191/2007) and the Immigration Regulations (LN 205/2004). The non-EU, EEA and Swiss regime grants two applications to third-country nationals; namely, CEA Form B and the key employee initiative, which is a single work permit for managerial or highly technical posts.

UPDATE AND TRENDS

Current developments

41 Are there any other current developments or emerging trends to note?

The main current development in Malta is the drive and effort with which the Malta Financial Services Authority, as a proactive financial services regulator, is promoting the idea of Malta becoming a global fintech hub. Throughout its long-term fintech strategy, the regulator is not only supporting the financial services industry to harness the opportunities presented by innovation and technology, but is also geared up to harness as much legal and regulatory certainty as possible for industry players to operate in an environment with effective investor protection, market integrity and financial soundness.

Read this article on Lexology

Leonard Bonello lbonello@ganado.com
James Debono jdebono@ganado.com

171 Old Bakery Street, Valletta VLT 1455, Malta
Tel: +356 21 23 54 06
www.ganadoadvocates.com

Read more from this firm on Lexology

Read this article on Lexology

Netherlands

Jeroen Bos, Koen van Leeuwen and Marise Kok
Simmons & Simmons

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 391
General innovation climate 391
Government and regulatory support 392

FINANCIAL REGULATION 393
Regulatory bodies 393
Regulated activities 393
Consumer lending 394
Secondary market loan trading 394
Collective investment schemes 394
Alternative investment funds 395
Peer-to-peer and marketplace lending 395
Crowdfunding 395
Invoice trading 396
Payment services 396
Open banking 397
Robo-advice 397
Insurance products 398
Credit references 398

CROSS-BORDER REGULATION 398
Passporting 398
Requirement for a local presence 399

SALES AND MARKETING 399
Restrictions 399

CRYPTOASSETS AND TOKENS 400
Distributed ledger technology 400
Cryptoassets 401
Token issuance 402

ARTIFICIAL INTELLIGENCE 403
Artificial intelligence 403

CHANGE OF CONTROL 404
Notification and consent 404

Read this article on Lexology

FINANCIAL CRIME	**404**
Anti-bribery and anti-money laundering procedures	404
Guidance	405
DATA PROTECTION AND CYBERSECURITY	**405**
Data protection	405
Cybersecurity	408
OUTSOURCING AND CLOUD COMPUTING	**410**
Outsourcing	410
Cloud computing	410
INTELLECTUAL PROPERTY RIGHTS	**410**
IP protection for software	410
IP developed by employees and contractors	411
Joint ownership	411
Trade secrets	412
Branding	412
Remedies for infringement of IP	413
COMPETITION	**413**
Sector-specific issues	413
TAX	**415**
Incentives	415
Increased tax burden	417
IMMIGRATION	**418**
Sector-specific schemes	418
UPDATE AND TRENDS	**421**
Current developments	421

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Fintech innovation in the Netherlands continues to develop. There has been a high level of activity in the fields of artificial intelligence, machine learning, blockchain, mobile and advanced analytics. The Dutch market is also adopting other innovations such as open banking (as a result of Directive (EU) 2015/2366 (second Payment Services Directive)).

Generally, diversification in the Dutch financial services sector has increased due to new entrants entering the market and incumbents (such as large Dutch banks) progressing their own fintech initiatives. However, increasing regulatory scrutiny and supervisory costs seems to deter new entrants into the market. Nevertheless, despite the additional administrative and compliance costs of the Dutch registration regime for certain crypto service providers that applies since May 2020, nearly 40 crypto service providers are registered to date.

Read this article on Lexology

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

In June 2016, the Dutch Authority for the Financial Markets (AFM) and the Dutch Central Bank (DNB) set up the InnovationHub to provide new and existing firms with support in answering queries related to the regulation of innovative financial products and services. The InnovationHub is a joint information desk of the AFM, DNB and the Dutch Authority for Consumers and Markets (ACM). It aims to offer easy access to supervisors and regulators for companies that provide innovative services or products, gain more insight into the rapidly developing technological innovation within the financial sector, and improve knowledge, sharing and dialogue with all relevant stakeholders. Firms can submit specific questions through the Innovation Hub, to which DNB, the AFM and the ACM provide informal answers.

In 2016, the AFM and DNB set up the Regulatory Sandbox for fintech companies to test and develop new products. If certain criteria are met, the Regulatory Sandbox can provide bespoke solutions for financial services companies that cannot reasonably meet specific policies, rules or regulations when marketing an innovative product, service or business model, but that do meet the underlying rationale of these policies, rules or regulations. The Regulatory Sandbox was evaluated as part of the discussions taking place in the iForum.

The DNB also periodically organises the Fintech meets the Regulator seminar, during which relevant market participants and the DNB share thoughts on current developments.

Additionally, in November 2019, the DNB launched the iForum, a platform for joint initiatives intending to create value for the Dutch sector and the DNB. Through the iForum, the Dutch sector and the DNB can have a dialogue on the impact of technological innovations on the sector and develop joint pilots and experiments.

In October 2021, the ACM, the AFM, the Dutch Data Protection Authority (AP) and the Dutch Media Authority (CvdM) established the Digital Regulation Cooperation Platform (SDT). The SDT wishes to gain more insight into the online use of personal data by algorithms, among other things, and will coordinate how to enforce (new) EU rules and regulations on digitalisation. For example, this includes new rules and regulations on dealing with large technology companies, the data economy and the platform economy (such as the Digital Services Act, the Digital Markets Act, the Data Governance Act and the Artificial Intelligence Act).

There are no formal arrangements with foreign regulators that relate specifically to fintech companies. However, both the AFM and the DNB maintain contact with other regulators in the Netherlands (such as the ACM, the AP and the CvdM), the European Union and globally (such as the International Organization of Securities Commissions).

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

There is no specific regulatory framework applicable to the provision of fintech products and services, besides the registration regime for certain crypto service providers. Such crypto-service providers are supervised by the Dutch Central Bank (DNB).

As such, depending on the nature and scope of products and services offered, the Dutch Authority for the Financial Markets (AFM) and the DNB supervise compliance with the conduct of business rules and prudential requirements respectively.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Depending on the nature and scope of services offered, licensing requirements under the Dutch Financial Supervision Act (FSA) and secondary legislation may apply.

The following activities are regulated under the FSA:

- deposit-taking and extension of credit for one's own account: credit institutions (ie, institutions that attract repayable funds from the public in the Netherlands and that extend credit for own account) require a banking licence.
- consumer lending: the extension of credit to consumers (natural persons acting outside their business or profession) requires a licence.
- factoring, to the extent this would constitute consumer lending.
- invoice discounting, to the extent this would constitute consumer lending.
- payment services: all institutions carrying out payment services as described in the Annex to Directive (EU) 2015/2366 (second Payment Services Directive) (PSD2), require a licence. A licence to act as a credit institution may also cover carrying out payment services.
- investment services: a financial institution is required to have a licence if it intends to provide investment services. These can be split into the following services, carried out in pursuit of a business or profession:

    - receiving and transmitting client orders relating to financial instruments (which includes bringing about deals in financial instruments);
    - executing client orders relating to financial instruments;
    - managing an individual's assets;
    - providing advice regarding financial instruments;
    - underwriting or placement with a firm commitment basis of financial instruments; and
    - placement without a firm commitment basis of financial instruments; and

- investment activities: a financial institution is required to have a licence if it intends to perform an investment activity. Investment activities can be split into three activities:

- dealing on one's own account (including foreign exchange trading);
- operating an organised trading facility; and
- operating a multilateral trading facility; and

- clearing and settlement: acting as a clearing and settlement institution requires a licence; and
- secondary market loan trading.

The registration regime for certain crypto service providers follows from the Dutch Money Laundering and Terrorist Financing (Prevention) Act. This regime only applies to crypto service providers that provide exchange services between fiat currencies and virtual currencies and (or) provide custodian wallet services for virtual currencies.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Under the FSA, consumer lending requires a licence. Consumer credit is considered a financial product. Advising a consumer on a financial product or providing intermediary services in relation to such a financial product is only permitted if the institution has obtained a licence from the AFM. Financial institutions may be exempted if they have another licence that permits consumer lending or advising consumers on financial products.

Before entering a loan agreement with a consumer, the financial institution must provide the consumer with relevant information relating to the financial product, so that the consumer is able to properly assess the product. In addition, credit assessment rules exist to prevent consumer over-indebtedness. These rules are part of the overarching requirement that lenders exercise due care when providing these services.

Secondary market loan trading

6 | Are there restrictions on trading loans in the secondary market in your jurisdiction?

Secondary market loan trading is only a regulated activity where it constitutes consumer lending.

Collective investment schemes

7 | Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

In the FSA, collective investment schemes can be an alternative investment fund, as defined in Directive 2011/61/EU (Alternative Investment Fund Managers Directive) (AIFMD), or an undertaking for collective investment in transferable securities, as defined in Directive 2009/65/EC Undertakings for Collective Investment in Transferable Securities Directive (UCITSD).

Read this article on Lexology

Under the AIFMD, an alternative investment fund is a vehicle with or without legal personality, which raises capital from investors with a view to investing it in accordance with a defined investment policy for the benefit of those investors. The AFM has confirmed that firms offering units in funds that invest in cryptocurrencies require a licence as an AIFM.

Whether a fintech company qualifies as a collective investment scheme depends on the exact nature of its business. For example, fintech companies that manage assets on a pooled basis on behalf of investors should give particular consideration as to whether they qualify as a collective investment scheme. On the other hand, fintech companies that provide advice or payment services may be less likely to constitute a collective investment scheme. Peer-to-peer lenders, marketplace lenders or crowdfunding platforms could potentially fall within the scope of the AIFMD, to the extent they would qualify as (managers of) collective investment schemes.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

Yes. Managers of alternative investment funds are regulated under the AIFMD, which has been implemented in the FSA.

Peer-to-peer and marketplace lending

9 | Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

There is no specific regulation of peer-to-peer (P2P) or marketplace lending in the Netherlands. However, this activity might constitute a regulated activity under the FSA. For instance, if a platform facilitating P2P lending receives and transmits orders in financial instruments, it may be subject to a licensing obligation as an investment firm.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

As of 10 November 2021, the EU Crowdfunding Regulation applies. Among other things, this Regulation introduced a licensing regime for crowdfunding service providers (CSPs) that:

- facilitate granting of loans excluding consumer credit (loan-based crowdfunding); or
- place without a firm commitment basis transferable securities and instruments issued by project owners or SPVs, and receive and transmit orders for crowdfunding purposes (equity-based crowdfunding).

However, if crowdfunding offers made by a particular project owner exceed €5 million over a period of 12 months, then the licensing regime for investment firms under Directive 2014/65/EU (Markets in Financial Instruments Directive II) (MiFID 2) applies instead.

CSPs that were permitted to provide crowdfunding services in the Netherlands before 10 November 2021 can avail themselves of a transitional regime under which they are permitted

to continue doing so until 10 November 2022. This transitional period has been extended by one year until 10 November 2023.

After this date, CSPs require a licence from the AFM under the EU Crowdfunding Regulation. The AFM encourages CSPs to already apply for such licence, regardless of the abovementioned extension of the transitional period.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

There is no specific regulation of invoice trading in the Netherlands. However, depending on the exact services provided and the status of the parties involved, invoice trading may lead to either party qualifying as an intermediary of consumer credit or may amount to the extension of consumer credit.

Payment services

12 | Are payment services regulated in your jurisdiction?

Yes. In the Netherlands, payment services are regulated based on PSD2, which has been implemented in the FSA. A licence is required to carry out all payment services listed in the Annex to PSD2.

Payment services include:

- services enabling cash to be placed on a payment account or cash withdrawals from a payment account and all the operations required for operating a payment account;
- the execution of the following types of payment transactions:
    - direct debits, including one-off direct debits;
    - payment transactions executed through a payment card or a similar device; and
    - credit transfers, including standing orders; and
    - the execution of the following types of payment transactions where the funds are covered by a credit line for the payment service user:
    - direct debits, including one-off direct debits;
    - payment transactions executed through a payment card or a similar device; and
    - credit transfers, including standing orders; and
    - issuing payment instruments or acquiring payment transactions;
    - money remittance;
    - payment initiation services (initiating a payment order at the request of a payment service user with respect to an account held with another payment service provider); and
    - account information services (online services to provide consolidated information on one or more payment accounts held by the payment service user with another one (or more) payment service provider).

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

The implementation in the FSA of the access-to-account rules, as included in the PSD2, requires financial institutions to provide access to the payment accounts of clients to payment initiation service providers and account information service providers. In general, data protection and privacy regulations should be considered prior to making client data available to third parties.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Currently, there is no specific regulatory framework for robo-advisers in the Netherlands.

As such, there is no legal distinction between robo-advice and traditional investment advice in the Netherlands. Therefore, companies providing robo-advice must – in principle – fulfil the same legal requirements as companies providing traditional investment advice.

However, the AFM has issued two documents relating to robo-advice:

- the AFM's view on robo-advice, in which the AFM discusses the duty of care and points of attention specifically in relation to robo-advice on mortgage loans and occupational disability insurance (but also in relation to other high-impact financial products). In general, the AFM states that while robo-advice could be an opportunity to improve both access and the quality of investment advice, there are also specific points of attention to consider, including:
    - determining for which target group robo-advice is suitable;
    - determining which financial products are included in the robo-advice;
    - the algorithm's ability to identify when clients have doubts;
    - detection of contradictory client answers; and
    - explanations on the product features and advice; and
- guidelines for (semi)-automated portfolio management, in which the AFM provides guidance regarding the (technique-neutral) duty of care of asset managers who offer semi-automatic investment advice and portfolio management. These guidelines are not legally binding but they do bring clarity for asset managers. The guidelines are aligned with Dutch law, MiFID 2 and suitability guidelines published by the European Securities and Markets Authority and set out, among other things, guidance on safety and the provision of information.

Additionally, on 1 July 2020, Dutch draft legislation on automated advice was published as part of a publication consultation. This legislation aims to introduce safeguards to ensure adequate provision of automated advice. In this context, the legislation:

- applies competence requirements to automated advice;
- requires that two individuals are responsible for the automated system and advice; and
- imposes rules on controls and systems.

This legislation targets automated advice on financial products in general. On 3 May 2023, the Dutch Council of State issued its advice on this draft legislation.

At this moment, there is no specific regulation of other companies that provides retail customers with automated access to investment products in the Netherlands. There is no legal distinction between companies providing automated access to investment products and companies that offer investment products in a traditional way.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Yes. The sale of insurance products is regulated under the FSA and requires a licence.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

The rules on credit rating agencies laid down in Regulation (EC) No. 1060/2009 on credit rating agencies (as amended) apply in the Netherlands. A credit rating agency is required to adopt, implement and enforce adequate measures to ensure that the credit ratings it issues are based on a thorough analysis of all the information that is available to it and is relevant to its analysis according to its rating methodologies.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

An EEA firm that has been authorised under one of the EU single market directives (Directive 2013/36/EU (Capital Requirements Directive), Directive 138/2009/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (Recast), Directive 2014/65/EU (Markets in Financial Instruments Directive II), Directive (EU) 2016/97 (Insurance Distribution Directive) (Recast), Directive 2014/17/EU (Mortgage Credit Directive), Directive 2009/65/EC Undertakings for Collective Investment in Transferable Securities Directive, Directive 2011/61/EU (Alternative Investment Fund Managers Directive) and Directive (EU) 2015/2366 (second Payment Services Directive) may, in principle, provide

cross-border services into or establish a branch in the Netherlands. This also applies to an EEA firm authorised as a crowdfunding service provider under Regulation (EU) 2020/1503 on European Crowdfunding Service Providers.

To exercise this right, in general, the firm must first provide notice to its home state regulator. The relevant directive under which the EEA firm is seeking to exercise its passporting rights as implemented in the Dutch Financial Supervision Act (FSA) will determine the conditions and processes that the EEA firm must follow.

Crypto service providers registered elsewhere in the EEA for the provision of exchange services between virtual and fiat currencies, and custodian wallet services currently cannot passport their services into the Netherlands.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

To obtain a licence for any of the activities regulated pursuant to the FSA; in general, a local presence must be established, unless a firm can benefit from a European passport or a specific cross-border licensing regime is available.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Depending on the regulatory status of the financial institution, different marketing rules may apply, including clientele restrictions. Advice should be sought on the specific circumstances of any particular case.

The Dutch Financial Supervision Act (FSA) states that, in general, relevant marketing activities:

- must be correct, clear and not misleading;
- must be recognisable as being of a commercial nature (where applicable); and
- may not contradict the information that is required to be made available pursuant to the FSA.

In addition, specific rules apply depending on the type of product offered or service provided and, in some cases, also on the type of client targeted. Some of these are summarised below.

Marketing materials for complex products (eg, participation rights in an open-ended collective investment scheme and investment objects) should include a risk indicator as prescribed by the Dutch Further Regulation on Conduct of Business Supervision of Financial Undertakings (the Further Regulation).

Read this article on Lexology

Marketing materials for credit offerings to consumers that refer to debit interest rates or other information regarding costs should include (at a minimum) information regarding floating or fixed interest rates and other costs that form part of the total costs of the credit for the consumer, the total credit amount, the yearly cost percentage, identity and address of the provider or intermediary, and certain other information depending on the type of credit, all as prescribed in the Decree on Conduct of Business Supervision of Financial Undertakings.

In addition, certain risk warnings are prescribed and certain prohibitions apply, such as the prohibition on including any references to the speed or ease with which the credit may be obtained.

For products other than complex products, general marketing rules included in the Further Regulation apply, including the obligation to include a warning that the value of an investment may fluctuate and that historical returns offer no guarantee for the future.

Depending on the medium used for marketing (print, TV, radio or internet) further rules apply, such as the relevant information to be included at a minimum (namely, the name of the provider, the regulatory status of the provider, and where and how further information relating to the product or service can be obtained). Specific marketing rules have been introduced to facilitate marketing on social media.

Further, the Dutch Authority for the Financial Markets (AFM) has imposed a ban on the selling, marketing or distribution of binary options to retail clients. It has also imposed restrictions with respect to the selling, marketing and distributing of contracts for differences to retail clients and turbos to retail clients (with respect to turbos, among others a leverage cap for such products with crypto as an underlying is imposed).

Finally, there is increasing attention from the AFM for the role of 'finfluencers' in promoting certain products or firms.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

Currently, no specific rules or regulations apply that govern the use of distributed ledger technology (DLT) or blockchain, other than Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology, which became applicable on 23 March 2023. This pilot regime lays down uniform requirements for firms that intend to operate a DLT infrastructure. DLT market infrastructures may only admit to trading or recording DLT financial instruments on a distributed ledger.

Firms that intend to operate under this pilot regime need to apply for a permission from the Dutch Authority for the Financial Markets (AFM) as a:

- DLT multilateral trading facility;
- DLT settlement system; or
- DLT trading and settlement system.

The pilot regime will, in any case, apply for a period of three years, after which an evaluation at the EU level will take place.

Generally, the use of DLT is subject to existing regulatory legislation (eg, the Dutch Financial Supervision Act (FSA)) depending on its application in any particular case. DLT is a topic that has led to many questions in the InnovationHub.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

The Dutch Central Bank (DNB) and the AFM have stated that digital currencies do not constitute a financial product (such as e-money or a financial instrument) and do not qualify as legal tender. Therefore, in principle, the FSA does not apply to digital currencies.

However, digital currencies may fall within the scope of the FSA on the basis of activities provided in relation to these currencies. For example, this would be the case when the holder of a digital wallet is able to convert its digital currency holdings into cash holdings held with the crypto-service provider. Further, depending on the structure and the specific characteristics of the digital currency or digital wallet, the relevant services could be considered to constitute payment services or e-money-related services. In these circumstances, unless an exemption applies, the relevant activities trigger a licence requirement under the FSA and certain prudential and conduct-of-business rules will apply.

Additionally, crypto service providers that provide exchange services between virtual and fiat currency or custodian wallet services in or from the Netherlands are required to register with the DNB.

On 24 September 2020, the European Commission published a draft Markets in Crypto-Assets (MiCA) Regulation.

Under the MiCA Regulation, currently, out-of-scope assets and service providers will be regulated. Under the MiCA Regulation, cryptoassets are categorised as e-money tokens, asset-referenced tokens and cryptoassets other than asset-referenced tokens and e-money tokens (including utility tokens). This categorisation also covers certain types of stablecoins.

Cryptoassets that are currently regulated (eg, as a financial instrument or e-money) will not fall within the scope of the MiCA Regulation. Also, unique NFTs for now will not fall within the scope of the MiCA Regulation (fractional NFTs and large NFTs collections will fall within scope).

Further, the MiCA Regulation will regulate certain cryptoasset services, including:

Read this article on Lexology

- the provision of custody services;
- the operation of a crypto trading platform;
- the exchange of cryptoassets for funds;
- the exchange of cryptoassets for other cryptoassets;
- the execution of client orders in cryptoassets;
- the placing of cryptoassets;
- the reception and transmission of client orders in cryptoassets;
- the provision of advice on cryptoassets;
- the provision of portfolio management on cryptoassets; and
- the provision of transfer services for cryptoassets.

In this context, the MiCA Regulation introduces a licensing requirement for firms providing the abovementioned cryptoasset services (crypto asset service providers (CASPs)). In addition, the MiCA Regulation introduces the requirement for issuers of certain types of cryptoassets to publish a white paper (setting out the core information on these cryptoassets) and a licensing requirement for issuers of asset-referenced tokens.

On 16 May 2023, the final step of the legislative process was taken by the adoption of the MiCA Regulation by the EU Council. It is the expectation that the MiCA Regulation will be published in the EU Official Journal by July 2023 at the latest, with entry into force 20 days after such publication. The MiCA Regulation will apply to CASPs 18 months following the date of entry into force and to issuers of certain cryptoassets 12 months following the date of entry into force.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

The DNB and the AFM have stated that digital currencies do not constitute a financial product (such as e-money or a financial instrument) and do not qualify as legal tender. Therefore, in principle, the FSA does not apply to digital currencies (unless these in specific circumstances do qualify as financial instruments). However, digital currencies may fall within the scope of the FSA on the basis of activities provided in relation to these currencies.

Further, crypto service providers that provide exchange services between virtual and fiat currency (eg, by operating a crypto exchange) in or from the Netherlands are required to register with the DNB.

Additionally, digital currency exchanges, crypto-brokers and issuers of cryptoassets may fall within the scope of the future MiCA Regulation.

Finally, the AFM warned regarding the serious risks associated with ICOs, such as their vulnerability to misrepresentation, fraud and manipulation, their potential use for the laundering of money obtained by criminal means and the possibility that investors may lose their entire investment. In this context, the AFM advises customers to avoid investing in ICOs.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

Currently, there is no specific regulatory framework for the use of artificial intelligence (AI). Nevertheless, both the Dutch Central Bank (DNB) and the Dutch Authority for the Financial Markets (AFM) pay particular attention to the use of AI. For example, in 2019, the DNB published general principles for the use of AI in the financial sector. The DNB and the AFM focus on the use of AI in the insurance sector, by among others conducting market research. Further, in its report Machine Learning in Trading Algorithms, published in March 2023, the AFM reminds the market of the risks related to the use of machine learning in proprietary traders' trading algorithms.

Also, on 21 April 2021, the European Commission published a draft Regulation on the use of AI. A draft negotiation mandate was adopted in the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs and Committee on the Internal Market and Consumer Protection on 11 May 2023. The purpose of this Regulation is to lay down rules for the development, marketing and use of AI.

Further, at the moment there is no specific regulation on automated investment advice. However, the AFM has issued guidelines regarding the duty of care of asset managers who offer semi-automatic portfolio management (and investment advice). These guidelines are not legally binding but they do bring clarity for asset managers. The guidelines are aligned with Dutch law, Directive 2014/65/EU (Markets in Financial Instruments Directive II) and suitability guidelines published by the European Securities and Markets Authority and set out, among other things, guidance on safety and the provision of information.

The AFM has published its views on robo-advice more generally, stating that while robo-advice could be an opportunity to improve both access and the quality of investment advice, there are also specific points of attention to consider.

However, on 1 July 2020, the Dutch draft legislation on automated advice was published as part of a publication consultation. This legislation aims to introduce safeguards to ensure adequate provision of automated advice. In this context, the legislation:

- applies competence requirements to automated advice;
- requires that two individuals are responsible for the automated system and advice; and
- imposes rules on controls and systems.

This legislation targets automated advising on financial products in general. On 3 May 2023, the Dutch Council of State issued its advice on this draft legislation.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

If a qualifying holding (at least 10 per cent of the shares or voting rights, or both) is obtained in certain Dutch financial firms (such as settlement institutions, banks, managers of undertakings for collective investment in transferable securities, investment firms, entities for risk acceptance, premium pension institutions, insurers, reinsurers, payment service providers and electronic money institutions), prior approval by the Dutch Central Bank (DNB) is required. In specific cases, increases in qualifying holdings above certain thresholds are also notifiable to or subject to approval from the DNB.

This also applies to any qualifying holdings in Dutch registered crypto service providers.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

There is no general framework under which fintech companies are required to have in place procedures to combat bribery or money laundering. Nevertheless, financial firms are generally subject to anti-money laundering and combating the financing of terrorism requirements.

Further, as of 21 May 2020, certain crypto service providers fall within scope of the Money Laundering and Terrorist Financing (Prevention) Act.

This concerns companies, legal entities or natural persons that provide:

- services for the exchange between virtual and fiat currencies; and
- services offering custodian wallets (namely, services to safeguard private cryptographic keys on behalf of customers; consequently, 'soft wallets' do not fall within the scope).

These crypto service providers are required to register with the Dutch Central Bank (DNB), to the extent they provide exchange services between virtual and fiat currency or custodian wallet services 'in or from the Netherlands'. A crypto service provider is providing services 'in the Netherlands' if it has directed its activities to the Dutch market (eg, marketing, use of the Dutch language, offering the possibility to pay via Dutch-specific payment methods (such as iDEAL) etc). Non-EEA crypto service providers are currently not eligible for registration with the DNB.

Requirements for such registration include (but are not limited to) having in place an adequate integrity policy to ensure ethical operation management. In this policy, an analysis

of integrity risks, compliance with the Dutch Sanctions Act, transaction monitoring, reporting of unusual transactions to the Financial Intelligence Unit-Netherlands and customer due diligence must be covered. Further, the DNB applies a 'wallet verification requirement' in relation to incoming and outgoing transactions in the context of sanctions screening.

Other requirements for registration include, among others, that:

- the policymakers of crypto service providers are trustworthy and suitable; and
- the (directors of) holders of a qualifying holding in (at least 10 per cent of the shares or voting rights, or both) and ultimate beneficial owners of crypto-service providers are trustworthy.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no regulatory or industry anti-financial crime guidance specifically for fintech companies. However, the Dutch Authority for the Financial Markets, the DNB and the Dutch Authority for Consumers and Markets have set up the InnovationHub to support market operators, such as fintech companies. The purpose of the InnovationHub is to provide new and existing firms with support in answering queries related to the regulation of innovative financial products and services.

Further, the DNB has published a brochure titled 'Good practices fighting corruption' and the DNB website provides answers to questions regarding the DNB's integrity supervision of crypto-service providers. As regards anti-money laundering and combating the financing of terrorism, the DNB issued a comprehensive guidance in December 2020 titled 'Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Dutch Sanctions Act', which is also relevant for payment service providers, e-money institutions and certain crypto service providers.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The transfer of personal data is subject to local and EU data protection laws (specifically the General Data Protection Regulation (GDPR)). On 25 May 2018, the GDPR came into force with direct effect across the European Union. It governs the storage, viewing, use of, manipulation and other processing by businesses of data that relates to a living individual. In summary, the GDPR requires that businesses may only process personal data where that processing is done in a lawful, fair and transparent manner, as further described in the GDPR.

The GDPR requires that any processing of personal data must be done pursuant to one of six lawful bases for processing. The most commonly used lawful basis for processing (outside an employment relationship) is the consent of the data subject to that processing. To have obtained valid consent, consent must be freely given, specific, informed, unambiguous and capable of being withdrawn as easily as it is given. Also, it must be made by way of a statement or clear affirmative action. This places a significant burden on businesses to ensure that their customers are fully informed on what their personal data is being used for, which is a crucial change to the previous regime under which disclosure did not need to be so transparent.

Organisations often engage other organisations to process personal data for them. For example, by using a cloud service that stores personal data. Such another organisation is called a processor. The organisation that engages the processor is the controller. Depending on the location of the processor, specific requirements apply to the transfer of data. If the processor is located in the European Economic Area, the transfer of data is permitted. The requirements of article 28 of the GDPR must be documented. Where a data processor carries out processing on behalf of a data controller, article 28 of the GDPR requires the parties to enter into a written agreement, which imposes specific obligations on the data processor.

If the processor is located outside the European Economic Area and data is transferred outside of the European Economic Area, the GDPR requires the controller to specify the condition relied upon for the international data transfer to ensure that the transferring personal data is afforded the same level of protection as applies to it in the European Economic Area.

A number of possible safeguards can be taken, such as:

- a transfer to an 'adequate' country, which is the simplest way to transfer personal data outside the European Economic Area. This is a formal decision made by the European Union, which recognises that another country, territory, sector or international organisation provides an equivalent level of protection for personal data as exists within the European Union;
- standard contractual clauses approved by the European Commission that can be adopted for the transfer of personal data to controllers and processors located outside of the European Economic Area;
- binding corporate rules; and
- derogations, which can only be relied on in the absence of an adequacy decision for the third country to which the data is to be transferred and derogations are limited to occasional transfers only.

This includes the onward transfers of personal data from a third country or an international organisation to another third country or to another international organisation (as stated in article 44 of the GDPR).

In the absence of an adequacy decision, or of appropriate safeguards, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions (as stated in article 49 of the GDPR):

Read this article on Lexology

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; and
- the transfer is made from a register, which according to Union or EU member state law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or EU member state law for consultation are fulfilled in the particular case.

Obtaining consent for non-EEA transfers is a derogation from the rule that data must not be transferred outside the European Economic Area unless the destination country provides an adequate level of protection or an adequate safeguard is in place. As a general principle, the derogation is limited to occasional transfers and is not intended to cover transfers that occur on a regular basis. The explicit consent (namely, an affirmative action) of the data subject, rather than just mere consent must be obtained, and consent must be specific to the transfer. The data subject must also be informed of the possible risks associated with such transfer. Guidance on this notes that if the controller does not have a specific transfer envisaged at the time of collection of the data it cannot ask for consent at that stage to a possible future transfer but must request it again once the circumstances are known. Further, a request for consent must be brought specifically to the data subject's attention and cannot be concealed or contained within a fair processing notice. This is because the GDPR imposes a high threshold for obtaining consent, namely that consent must be freely given, informed, specific and unambiguous. On this basis, the fair processing notice would not suffice in itself. The level of consent required is even greater than in relation to standard GDPR processing, as data exporters must make additional efforts to make data subjects aware of the risks of transferring to third countries, and therefore would not be a feasible long-term solution.

The laws of the country where the data is transferred will also apply to that personal data when it arrives in that country. The Dutch General Data Protection Regulation (Implementation) Act (UAVG) does not impose any additional requirements on the transfer of data to third countries outside the European Economic Area other than those already listed above.

The GDPR further differs from the previous regime in that it places a significantly increased compliance burden on businesses, including, for example, mandatory requirements to notify regulators of data breaches, obligations to keep detailed records on processing and requirements for most entities to appoint a data protection officer. Businesses that infringe the GDPR may be subject to administrative fines of an amount up to €20 million or 4 per cent of global turnover, whichever is higher.

Read this article on Lexology

Personal data can be pseudonymised and anonymised. In the first case, personal data is still personal data, in the second case it is not. Recital 26 of the GDPR states that where data has been processed such that it is truly anonymised, the principles within the GDPR do not apply to the processing of that data. When personal data is processed and this data is anonymised, the UAVG no longer applies to that anonymised data. However, the anonymisation of personal data itself does constitute a processing operation to which the UAVG fully applies. Anonymous data means data that cannot be traced back to an identified or identifiable natural person.

The Article 29 Working Party has released Opinion 05/2014 on Anonymisation Techniques (in the context of the previous EU data protection regime). This Opinion discusses the main anonymisation techniques used – randomisation and generalisation (including aggregation). The Opinion states that when assessing the robustness of an anonymisation technique, it is necessary to consider:

- if it is still possible to single out an individual;
- if it is still possible to link records relating to an individual; and
- if information can be inferred concerning an individual.

In relation to aggregation, the Opinion further states that aggregation techniques should aim to prevent a data subject from being singled out by grouping them with other data subjects. While aggregation will avoid the risk of singling out, it is necessary to be aware that linkability and inferences may still be a risk with aggregation techniques.

The position on anonymisation taken from the Article 29 Working Party's Opinion is broadly unchanged in the GDPR. The GDPR itself also gives limited guidance on anonymisation in Recital 26, requiring data controllers to consider a number of factors in deciding if personal data has been truly anonymised, including the costs and time required to de-anonymise, the technology available at the time to attempt de-anonymisation and further technological developments that may take place.

Further, there are no legal requirements or regulatory guidance relating to personal data that are specifically aimed at fintech companies.

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

Directive (EU) 2015/2366 (second Payment Services Directive) (PSD2) includes provisions relating to measures that should be implemented by payment institutions, such as securing the payment service user's personal security data and agreeing on how to manage operational and security risks. Annually, payment service providers must file a report to the Dutch Central Bank (DNB). The report needs to contain an assessment of operational and security risks relating to the payment services provided. In addition, the report needs to address the adequacy of the financial institution's mitigating measures and control measures.

Second, payment service providers must notify the DNB of any major operational or security incidents within four hours after detection. If the incident (possibly) impacts the financials of the users, the payment service must notify them about the incident, without undue delay.

Read this article on Lexology

Last, the payment service provider must inform users of the measures taken to mitigate the damaging effect of the incident.

In addition to the PSD2, the Security of Network and Information Systems Act requires that certain fintech firms report serious digital security incidents to the National Cyber Security Centre. These are fintech firms that have at least 50 or more employees and (or) generate a revenue of at least €10 million and provide essential services (eg, energy, banking, financial markets infrastructure).

Further, Regulation (EU) 2022/2554 (Digital Operational Resilience Act) (DORA) came into force on 1 January 2023. It aims to harmonise IT regulations for the industry and further strengthen digital resilience. DORA imposes requirements on financial firms with regard to IT risk management, IT incidents, periodic digital resilience testing and risk management when outsourcing to IT service providers. Additionally, arrangements for sharing information on cyber threats have been developed. As of January 2025, DORA will apply to, among others, financial firms.

Among other things, DORA contains the following requirements:

- firms are expected to have an ICT risk management framework that detects and mitigates risks, and that this risk management is appropriately recorded. Enterprises should also conduct an annual risk assessment and set up business continuity processes.
- firms are expected to manage, classify and handle incidents and significant cyber threats in a process-based manner. It also prescribes, among other things, that regulators should be actively informed about the handling of critical IT incidents.
- firms must have a programme for testing their digital resilience.

Finally, the GDPR includes a few provisions relating to the security of processing, such as the requirement for the controller to, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures that are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing to meet the requirements of the GDPR and protect the rights of data subjects. The controller and the processor must also implement these measures to ensure a level of security appropriate to the risk, which may include, among other things:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Read this article on Lexology

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Where a financial services company outsources a material aspect of its business, it remains responsible for the outsourced activities. Further, outsourcing must not obstruct supervision by the authorities, and outsourcing by financial firms of critical or important functions must be notified to the regulator.

If a financial service provider plans on using a third party for activities for which a licence is required, this can only be done where both parties have a licence for these activities. For certain activities (such as fund management, investment services, payment services and elements of the CDD process under the Dutch Money Laundering and Terrorist Financing (Prevention) Act) further detailed outsourcing provisions apply.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

If a financial institution wants to make use of cloud computing, it must notify the Dutch Central Bank (DNB) of its intention to do so, regardless of the materiality of the outsourced activities. Before using cloud computing, the financial institution is required to develop a risk analysis, which must be presented to the DNB. Because the DNB qualifies cloud computing as a specific type of outsourcing, the rules on outsourcing apply. In addition, the DNB expects that the EBA recommendations on outsourcing to cloud service providers are taken into consideration.

Outsourcing is not allowed in cases where it would obstruct the supervision of the outsourced activities or where the internal audit function would be negatively affected by the outsourcing of the activities. Further, the financial institution is required to have adequate policies and proper procedures to manage outsourcing risks.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Computer programs (and preparatory materials) are protected by copyright. Copyright arises automatically as soon as the computer program is created, registration is not required. Copyrighted works are protected until 70 years after the death of the creator.

Databases underlying software programs may also be protected by copyright and, in certain circumstances, by database right. A database right is a stand-alone right that protects databases that have involved a substantial investment in obtaining, verifying or presenting their contents. The right automatically comes into existence upon creation and expires after 15 years.

Software may also be protected as confidential information or as a trade secret by keeping the software code secret. There are no formal (registration) requirements other than that a trade secret holder needs to take reasonable measures to protect its secret and it needs to have commercial value.

Computer programs and schemes, rules or methods of doing business as such are expressly excluded from patentability under the Dutch Patent Act 1995 and the European Patent Convention. However, patent protection for software may be possible if the inventor is able to demonstrate that the software makes a novel and inventive technical contribution over and above that provided by the computer program or business method itself. To obtain patent protection, registration is required with the relevant Dutch and European patent offices and the registration requirements must be followed. Patent protection is limited to 20 years starting from the date of filing the application.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Copyrights and databases created by an employee during the course of his or her employment are automatically owned by the employer unless the parties have agreed otherwise. Patents protecting inventions made by an employee in the course of his or her normal duties are owned by the employer. Any other patented inventions will be owned by the employee unless agreed otherwise.

Inventions or copyrights created by contractors or consultants in the course of their duties are owned by the contractor or consultant unless otherwise agreed. By contrast, database rights are owned by the person who takes the initiative and assumes the risk of investing in obtaining, verifying and presenting the data in question. Depending on the circumstances, this is likely to be the business that has retained the contractor or consultant.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Where two or more persons jointly own an intellectual property right, any one of them may use and enforce the right, unless otherwise agreed. Each joint owner may assign or charge its share of the intellectual property right without the other owners' consent. Exploitation of the intellectual property right, including the granting of licences and charging or assigning the intellectual property right, can only be done by the joint owners of the intellectual property right.

Read this article on Lexology

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

In the Netherlands, trade secrets are protected by the general law of tort (such as breach of the rules of fair competition) and by the Dutch Trade Secrets Act, which entered into force on 23 October 2018 and implements Directive 2016/943/EU (Trade Secrets Directive). The Trade Secrets Act provides more specific rules for the protection of trade secrets. The Trade Secrets Act defines a trade secret as information that:

- is secret, in the sense that it is not generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question;
- has commercial value because it is secret; and
- has been subject to reasonable steps by the holder of the information to keep it secret.

The Trade Secret Act contains measures and remedies to enforce trade secrets. The secret holder can claim an injunction against further use or disclosure of a trade secret. This includes injunctions against infringing goods, which are goods, the design, characteristics, functioning, production process or marketing of which significantly benefit from trade secrets unlawfully acquired, used or disclosed. The Trade Secret Act includes the possibility for the court to grant the winning party a full cost award of all reasonable and equitable legal costs and other costs.

Measures are available in the Netherlands to prevent public disclosure of trade secrets during court procedures. For example, the court may order oral hearings to be conducted 'behind closed doors' and hand down decisions in which confidential information is redacted. The current Trade Secret Act proposal includes a new rule introducing the option for the court to impose a confidentiality club, limiting the access to trade secrets.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brands can be protected as registered trademarks either in the Benelux alone (as a Benelux trademark) or across the European Union (as an EU trademark). Certain branding, such as logos and stylised marks, can also be protected by design rights and may also be protected by copyright. Design rights and trademarks are obtained by registering the design or trademark with the relevant authority (eg, the Benelux Office for Intellectual Property, World Intellectual Property Organization or European Union Intellectual Property Office).

The Benelux and EU trademark databases can be searched to identify registered trademarks or applications for a trademark with effect in the Netherlands. It is highly advisable for new businesses to conduct trademark searches to check whether earlier registrations exist that are identical or similar to their proposed brand names.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

As a preliminary point, on 1 June 2023, the new Unified Patent Court (UPC) commenced. The UPC offers a single, specialised patent jurisdiction for participating EU member states. The UPC has a court of first instance, which is divided into local divisions. The Netherlands will host one of these local divisions. For European patents that designate the Netherlands and are not opted out of this new system, it is also possible to litigate these in the Dutch local division of the UPC.

For the sake of completeness, we note that the below is meant as a listing of remedies available in the Dutch national courts for IP infringements (although these remedies are also available within the UPC).

Remedies available in the Dutch national courts include:

- preliminary and final injunctions (preliminary injunctions are available cross-border);
- damages or surrender of profits;
- delivery up or destruction of infringing products;
- orders to disclose certain information that relates to the infringement;
- publication orders; and
- reimbursement of costs, including court fees and costs of (patent) attorneys and experts (cost orders in Dutch intellectual property litigation are based on guidelines that provide fee caps for compensation that can be awarded in different types of proceedings. The highest fee cap is for highly complex patent litigation in the first instance, for which the fee cap is €250,000. In special circumstances, the courts may deviate from the fee caps in the guidelines).

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

The Dutch Authority for Consumers and Markets (ACM) continuously monitors compliance with competition law by companies active in all sectors and also including the financial sector. By means of the Financial Sector Monitor, the ACM carries out economic research into the operation of the financial markets and analyses the risks to competition. In previous years, the ACM presented its findings on competition in this respect. Further, the ACM has specific powers regarding payment system providers and interchange fees.

In 2016, the ACM called for public input on how it can help to boost fintech companies' contribution to competition in the financial sector whereby it indicated it would pay special attention:

- to barriers to entry that prevent the fintech sector from reaching its full potential; and
- to risks involved with rapid technological change that may have adverse effects on competition and innovation.

Following this communication, the ACM has so far looked into the following two specific issues:

- whether regulatory costs constitute barriers to entry for fintech companies. The ACM ordered a study from EY that concluded that such regulatory costs do not constitute obstacles for new providers in the financial sector; and
- whether banks are limiting access of fintech companies – front-end providers and end-to-end providers – to bank accounts and thereby hinder competition in the payment market.

The ACM identified a risk of foreclosure of front-end providers. As a result, the ACM announced that it will actively monitor the behaviour of banks and how they deal with requests for access. In addition, the ACM:

- proposed that where possible, in light of Directive (EU) 2015/2366 (second Payment Services Directive) (PSD2) and the European Commission's Regulatory Technical Standards, further national implementation of EU law regarding access to bank accounts should enable such access;
- indicated that a system of free access could result in the banks refusing access (which implies that the ACM proposes to allow the banks to ask for compensation for the costs related to providing access); and
- proposed that a light version of the banking licence could be created for fintech companies so that they can offer payment accounts.

As regards end-to-end providers, the ACM considered that the risks of foreclosure were limited. Nevertheless, it proposed to cut the red tape – in addition to the above-mentioned light banking licence:

- by defining objective permit criteria that are related to the actual risks posed by end-to-end providers; and
- by making sure that, in the development of instant payments infrastructures in Europe, fintech companies are able to directly participate in the systems and arrangements for clearing and settlement of payments under non-discriminatory and objective condition

In 2020, the ACM – on request of the Ministry of Finance – conducted a market study into the role of Big Tech (Amazon, Ant Group, Apple, Facebook, Google and Tencent) in the Dutch payment market and more specifically on the segments counter payments, online payments and payments between consumers. In this study, the ACM concluded that the presence of Big Tech at the time was limited but that it is growing and that Big Tech primarily offered consumers innovative means of payment (citing the use of smartphones for payment or the recent entry of Apple Pay on the counter payments segment). The ACM expected the presence of Big Tech, as well as the use of such payment methods by consumers, to increase in years to come and noted that these companies choose to offer payment services to reinforce their ecosystems, rather than being driven by the introduction of PSD2.

The ACM identified the following competition risks:

Read this article on Lexology

- access restrictions for new innovative players such as Big Tech and fintechs; and
- Big Tech leveraging its dominant market position in neighbouring markets to tip the payment market (through self-preferencing).

The ACM concluded that an amendment of PSD2 may be to ensure that it also applies to Big Tech as gatekeepers to ensure a level playing field for competitors and a free choice for consumers. The ACM in this respect also fully supports the European Commission's Digital Markets Act, which creates various obligations and prohibitions for certain digital services companies (gatekeepers).

In 2021, after having received complaints from dating-app providers, the ACM concluded that Apple abused its dominant position. The ACM determined that if an app provider offers digital content or services within the app for a fee, the app provider is required to agree to additional contractual conditions set by Apple.

These conditions required app providers to use Apple's payment system for the processing of payments and stipulated that app providers are not allowed to refer within their own apps to payment options outside the app, for example, to alternative payment options that app providers offer on their websites. According to the ACM, this constituted an abuse of a dominant position. The ACM, therefore, ordered Apple to change its conditions and imposed an order subject to periodic penalty payments. After incurring the maximum penalty payment, Apple changed its conditions and now allows different methods of payment in dating apps in the Netherlands. In view of the ACM, Apple now meets the requirements that the ACM sets under EU and Dutch competition rules.

In 2022, the ACM requested the Ministry of Finance to fix a flaw in the national legislation implementing the PSD2. Because of this flaw, the ACM could only take action if a payment institution had been granted a licence by the Dutch Central Bank. The ACM could not handle complaints or reports about banks filed by payment institutions that had been granted licences from other EU regulators. As a result, the ACM was unable to conduct effective oversight over Dutch banks that refuse to offer a bank account to payment institutions, such as fintechs, from other EU countries. To fix this flaw, the national legislation was amended in 2023.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

Investing in the fintech sector is encouraged by the Dutch government. Two main tax incentives are available for fintech companies and investors in the Netherlands, being of the innovation box regime and the research and development (R&D) wage tax rebate.

Innovation box regime

Dutch taxpayers may claim a particular tax treatment providing for an effective corporate income tax rate of 9 per cent instead of the statutory rate of 25.8 per cent (2023 rates) on profits realised in respect of certain intangible assets, such as patents, developed by the taxpayer (the innovation box). The regime applies insofar as the total income from the intangible assets to which the regime applies exceeds the total R&D costs for these assets. Further, the Netherlands applies a nexus approach limiting the benefits of the regime if R&D activities are outsourced to related parties. Software can also qualify as an intangible asset.

Wage tax deduction incentive to invest in R&D

- The R&D tax rebate (wage tax deduction (WBSO)) offers compensation for part of a company's R&D wage costs, other costs, and expenditures. In practice, the WBSO provides for a reduction in payroll taxes to be withheld from the salary of employees engaged in R&D in the Netherlands. As a result, the WBSO decreases a company's personnel costs providing a liquidity benefit to the employer.
- The WBSO amounts to 32 per cent of the first €350,000 of R&D wage and other costs and expenses, and 16 per cent of all further R&D costs and expenses. For start-ups, the tax deduction for the first €350,000 spent on R&D is 40 per cent (2023 rates).

Accelerated deprecation for corporate income tax purposes

In addition to the abovementioned innovation box regime and the WBSO, special tax incentives are available in the Netherlands to stimulate sustainable entrepreneurship. An investment rebate is a tax incentive in the form of an additional deduction amounting to a certain percentage of the investment made. Currently, there are several investment rebates available in the Netherlands. These investment rebates are:

- the small-scale investment rebate (KIA);
- the energy investment rebate (EIA); and
- the environmental investment rebate (MIA).

With respect to the EIA, an additional extension is provided for the flexible depreciation of qualifying investments (VAMIL).

The KIA is applicable when a maximum of €353,973 (amount for 2023) is invested in any relevant financial year. The KIA is not limited to sustainable investments but is generally applicable. To encourage investments in efficient energy assets, the EIA amounts to 45.5 per cent of the investment in 2023. The EIA applies subject to certain conditions. In 2023, the MIA allowance amounts to 45, 36, or 27 per cent of the investment amount.

Other than the above-mentioned investment rebates, the VAMIL does not create an additional deduction in the corporate income tax return, but provides for a temporary difference by allowing accelerated depreciation on assets in one year up to a maximum of 75 per cent. The remaining 25 per cent is depreciated on a straight-line basis.

Read this article on Lexology

Tax treatment of stock options

As of 1 January 2023, the tax treatment of employee stock options has changed as per that date the taxable moment for payroll withholding tax purposes due on stock options on (non-tradable) shares awarded to employees is deferred to the moment the shares become tradable. This change was introduced to attract and retain employees and make the Netherlands more competitive for start-ups and scale-ups providing by providing a (temporary) liquidity benefit. However, at the employee's discretion, taxation can still take place at the moment of exercise of the stock option as was the case under the old legislation.

Before implementation of the legislative proposal, payroll withholding taxes were to be withheld if an employer granted stock options to an employee at the moment when the employee exercised or sold the stock option. The taxable base consisted of the fair market value of the stock option at that moment. Due to the legislative change, the taxable moment for payroll withholding tax purposes is by default deferred to the moment the shares become tradable unless the employee opts for taxation at exercise. In the latter situation, any increases in value after the moment of taxation will not be subject to wage tax, and any benefits derived, most notably dividends, are not taxable as wages.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

Directive on a minimum effective tax rate of 15 per cent

Pillar 2, an initiative by the OECD/G20 Inclusive Framework, introduces a minimum level of taxation for multinationals with an annual consolidated revenue of at least €750 million. In scope, multinationals will at all times pay a minimum effective tax rate of 15 per cent on their worldwide profits, whereby their tax base is determined by reference to a multinational enterprise's financial accounts income after certain tax adjustments have been applied.

The European Commission published a directive proposal along the lines of the OECD Pillar 2 proposal. Adoption of the directive proposal requires a unanimous decision from all EU member states. Directive (EU) 2022/2523 (Pillar 2 Directive) was published in the Official Journal of the European Union on 22 December 2022. Currently, the intention is that EU member states need to implement the Pillar 2 Directive by 31 December 2023. On 24 October 2022, the Dutch legislator published a draft legislative proposal for the implementation of Pillar 2 and will prepare a final legislative proposal, to be submitted for approval to the Dutch parliament.

Under Pillar 2, a top-up tax should typically be due if the effective tax rate of the multinational enterprise group is lower than the minimum tax rate of 15 per cent. The primary mechanism for the implementation of Pillar 2 will be an income inclusion rule (IIR) pursuant to which additional top-up taxes are payable by a parent entity of a group if one or more constituent members of the group have been undertaxed. A secondary fall-back is provided by an undertaxed payment rule (UPR) if the IIR has not been applied. The UPR can be applied by:

1 limiting or denying a deduction for payments made to related parties; or

2 making an adjustment in the form of an additional tax.

In the Dutch draft legislative proposal published on 24 October 2022, the Netherlands opted for option (2).

Thirty per cent facility for expats capped at WNT standard

Under the 30 per cent facility, certain employees recruited from abroad to work in the Netherlands can receive a maximum of 30 per cent of their wages tax-free. The Dutch government plans to cap the 30 per cent facility as of 1 January 2024 for expats at the WNT standard (the maximum allowed income in the public-service sector). In 2023, this standard was set at an income of €223,000 per annum. Transitional rules may apply.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

The following are the most common corporate immigration schemes in the Netherlands (only relevant for non-EU, EEA and Swiss nationals – third-country nationals – since all EU, EEA and Swiss nationals are free to reside and perform any activities in the Netherlands as long as they wish since there is free movement of workers within the European Union, which is expanded to the EEA and Switzerland).

- Knowledge migrant scheme (highly skilled migrant scheme): this has nothing to do with knowledge as such, but everything with the gross monthly salary (exclusive of holiday allowance, normally 8 per cent of the salary) that is consistent with Dutch salary standards and with thresholds for 2023 that vary from €2,631 to €5,008 per month, depending on age or graduation date in the past three years before applying for such a residence permit from a Dutch or top 200 university from a master's degree or PhD (if graduation is from a university in the Netherlands then bachelor level is also allowed). In addition, the offered salary needs to conform with the prevailing market (namely, normal for the job title). These salary thresholds are indexed each year. However, this does not mean that the salary of the employee needs to change every year. In principle, changes need to be made when the validity of a residence permit is extended, the employee changes employer or the employee changes the purpose of the residence permit. In addition to the aforementioned, the formal employer in most cases needs to hold the status of a recognised sponsor for the purpose of regular labour and knowledge migrants. If the employer is not a recognised sponsor, the employer can apply for that or make use of a payroll company that is a recognised sponsor. The formal employer would borrow their recognised sponsorship, in which case the payroll company would be the formal employer and second the employee to the factual employer. The employer is also able to become a recognised sponsor by submitting an application to the Immigration and Naturalisation Service (IND); as a result, the employer will be considered a reliable partner of the IND.

- Intra-corporate transfer scheme (Directive 2014/66/EU (Intra-Corporate Transit Directive)): if the employee is a specialist, manager or trainee and remains on the payroll of his or her employer outside the European Union, and the employee was already employed at that entity outside the European Union within the same group of companies, he or she may be transferred to the Netherlands under the intra-corporate transfer scheme for up to three years for a specialist or a manager and for up to one year for a trainee (after which he or she can return to the country from where he or she was seconded, or the residence permit can be changed into, eg, a residence permit as a knowledge migrant provided that the salary criterion is met and the employer is a recognised sponsor). The validity of a residence permit as an intra-corporate transferee cannot be extended if, with that extension, the maximum duration of one (trainee) or three (specialist or manager) years is exceeded). No salary thresholds are applicable but the salary criterion for knowledge migrants is an indication, albeit that the salary needs to conform with the prevailing market and, of course, complies with the Dutch minimum wage Act. Also, no recognised sponsorship is required, but is nevertheless advisable for a faster procedure. As a recognised sponsor, the application procedure should just take two weeks instead of 90 days. Some form of intra-EU mobility is possible for a long or a short term, which for a short term would not lead to needing another work permit in the other EU country where the employee is temporarily transferred within the same group of companies. This scheme takes precedence over other schemes if the application or situation falls within the scope of the directive. There is also a national intra-corporate transfer scheme; however, with this Directive and the national knowledge migrant scheme, the national intra-corporate transfer scheme is not used that often as there are more requirements to be met.
- EU Blue Card scheme (Directive 2009/50/EC (Blue Card Directive): the EU version of the Dutch knowledge migrant scheme but with a higher salary threshold, and where specific education requirements apply. Foreign degrees must be rated by Nuffic. The salary threshold in the Netherlands is €5,867 gross per month, exclusive of holiday allowance for 2023. This salary threshold is indexed each year. Recognised sponsorship is not required but is nevertheless advisable due to the more rapid application procedure. The EU Blue Card can be issued for a maximum of four years (depending on the duration of the employment agreement but the employment agreement needs to be for at least one year). After this period, it is possible to renew the EU Blue Card, provided the conditions are met. This scheme remains unpopular in the Netherlands due to the much more flexible national knowledge migrant scheme. The Blue Card does have one advantage: if an employee has a Blue Card that is valid for at least 18 months in another EU country, that employee is already allowed to start working in the Netherlands under the condition that within one month of arrival in the Netherlands, a Dutch EU Blue Card is applied for and in some situations, a permanent residence permit can be applied for earlier than five years.
- International trade regulation: a scheme that may come in handy in certain situations where larger and mostly lower-paid groups of third-country nationals have to come to the Netherlands in the framework of a certain project that has been assessed and approved by the Dutch Employee Insurance Agency (UWV). The salary threshold is the Dutch statutory minimum wage, that on 1 July 2023 increased to €1,995 gross per month, exclusive of an 8 per cent holiday allowance. To qualify for the international trade regulation, there must be a time-defined trajectory of initially a maximum of three years, and there must be a relationship between the company in the Netherlands and abroad. The workers (employees, clients or director-major shareholders) must come to

Read this article on Lexology

the Netherlands to perform specialist or managerial duties. The work done may not be of a competitive nature (priority labour supply). This is assessed, among other things, on the basis of the nature, duration and value of the trajectory and nature of the work. Once the trajectory has been approved, the workforce only needs to be notified via a form of the UWV, and the workforce can start work immediately. No recognised sponsorship is necessary.

- Short-term knowledge migrant scheme: this has the same salary criteria as the above-mentioned criteria for the knowledge migrant scheme, but varying from €3, 672 to €5,008 gross per month exclusive of holiday allowance and the job in the Netherlands must be a specialist, key, scientific or managerial position. A work permit as a short-term knowledge migrant can be applied for by the employer at the UWV, the recognised sponsor, for short-term assignments for a maximum duration of three out of six months, limited by the duration of the Schengen visa or the free-term requirements of a maximum of 90 out of 180 days.
- The delivery of goods including assembling, repairing, installing, amending and instructing on the use of those goods, which includes software. This is an exemption in Dutch migration law. No work permit is needed for such work if that work is regarded as incidental labour. In this regard, incidental labour means that the work that needs to be done does not take longer than 12 consecutive weeks within 36 weeks. There is no specific salary criterion, but a salary must be consistent with Dutch salaries for similar work. Should the work, however, not fall within the scope of this exemption, there is also a single permit (that combines a work and residence permit) for the assembly and repair of equipment supplied by foreign companies. The personnel costs must, in that case, not be higher than the to-be-delivered goods, the work must not exceed a period of one year and the workers would need to have specific knowledge to finalise the delivery of the goods for the customer to be able to use the goods. In addition, the following activities are also excluded from the obligation for a work permit, (incidental labour): holding business meetings or concluding agreements with companies and institutions for a maximum period of 13 weeks within a 52-week period and receiving training for a maximum of 12 consecutive weeks within a 36-week period. Note that if the person concerned is going to work, a work permit must be applied for at the UWV, such as a work permit for a knowledge migrant short stay (the short-term knowledge migrant scheme).
- Researcher (Directive 2016/801/EU (Students and Researchers Directive): mostly for researchers and scientists working at universities and other research institutions and companies. A specifically recognised sponsorship is necessary for the purpose of educational institutions. The researcher will work as either a paid researcher, an unpaid researcher with a grant or a PhD candidate and complies with the admittance requirements. Other specific requirements are applicable. The researcher must have at least €1,354.08 gross per month exclusive of holiday allowance as income (salary, scholarship or grant, or in his or her bank account) to comply with the sufficient means of subsistence requirement.
- Intra-EU service provision: exempted from the work permit obligation in the Netherlands if intra-EU service provision is performed under articles 56 and 57 of the Treaty on the Functioning of the European Union, meaning that the work of third-country nationals in the Netherlands by a company based in an EU member state is allowed to provide services to companies in the Netherland. Note that this is only allowed if the third-country nationals are also allowed to conduct similar work in the country of residence. A residence permit obligation in the Netherlands applies after 90 out of 180 days for the

Read this article on Lexology

third-country national. Based on the third-country national's residence permit issued by the authorisation of another EU member state, this person can stay for 90 out of 180 days in the Netherlands. At day 91, a Dutch residence permit as a cross-border service provider is required. This residence permit at this moment has a maximum duration of two years. This is specifically for third-country nationals living and working legally in EU member state A who temporarily perform services or work for their employer in member state B. No salary threshold applies and no recognised sponsorship is needed. Alongside this, as of 1 March 2020, all cross-border service providers need to notify all their employees (including EU, EEA and Swiss nationals) via www.postedworkers.nl before starting to provide services in the Netherlands. Failure to notify on time will lead to a fine.

- Several specific training and trainee schemes. These are the most common schemes for corporate migration out of approximately 40 schemes available in the Netherlands, some based on EU law, some purely based on national law. Every case needs to be assessed by an immigration specialist on an individual basis since a different scheme to those stated above might be better suited. Further, there are several short-term work permit exemptions (incidental labour in the Netherlands), for example, for business meetings, receiving training courses or instructions regarding the use of goods manufactured in the Netherlands and services to be provided in the Netherlands. Living legally in the Netherlands is different from working legally in the Netherlands. It is, in principle, forbidden for a third-country national to perform any work in the Netherlands without a work permit, a work permit exemption or a Dutch residence permit with the suitable labour market annotation or single permit, except for very specific exemptions. Sanctions in the case of non-compliance are high – normally an €8,000 fine per illegally working foreigner and per employer in the meaning of the Dutch Foreigners Employment Act – but in most cases of an administrative rather than a criminal nature, additional sanctions may apply including shutting down the business operation in the Netherlands by up to three months.

Since 1 January 2021, UK nationals also need to fulfil the same criteria as any other non-EU, non-EEA citizen or non-Swiss national, as they have become third-country nationals.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

EU developments

Significant current developments relating to fintech seem to be driven at the EU level as a result of EU member states' adoption of the Digital Finance Package in September 2020.

Among other things, the Digital Finance Package introduces the MiCA Regulation (adopted by the EU Council on 16 May 2023, the Regulation is a pilot regime for infrastructure based on distributed ledger technology (which became applicable on 23 March 2023), and Regulation (EU) 2022/2554 (Digital Operational Resilience Act), which will apply as of January 2025). Further, the European Commission published a draft Regulation on the use of artificial

intelligence in April 2021 (in respect of which a draft negotiation mandate was adopted by the EU Parliament's relevant Committee on 11 May 2023) and its anti-money laundering and combating the financing of terrorism (AML/CFT) Reform Package in July 2021. The latter will have a significant impact on crypto service providers as it among others brings crypto transfers into the scope of the EU Transfer of Funds Regulation (as endorsed by the EU Council on 16 May 2023) and introduces an EU Regulation on AML/CFT requirements.

Additionally, on 1 June 2023, the Unified Patent Court (UPC) commenced. The UPC is the most significant change in European patent law in 50 years. It offers a single, specialised patent jurisdiction for participating EU member states. It enables patentees to enforce all designations of a European patent in one single enforcement action at the UPC.

With the UPC, patentees also have the option of applying for unitary patents, which will have effect across all participating EU member states. So far, 17 EU member states have ratified the necessary legislation, and 24 are currently signatory states. Signatory states that have not ratified yet can do so at any time. The unitary patent may provide significant cost advantages and a significant reduction of administrative burdens for patentees that normally validate their patents in multiple EU countries.

Finally, in 2022, both the Digital Services Act (DSA) and the Digital Markets Act (DMA) entered into force, which are also relevant for fintech companies. The DSA imposes multiple obligations (most notably transparency and terms of service requirements) on online service providers, including platforms, whereas the DMA creates various obligations and prohibitions for certain digital services companies (gatekeepers). It is unlikely that a fintech company will be designated as a company falling under the DMA or DSA. However, fintech companies, as beneficiaries of these acts, can enforce compliance with obligations by their service providers, such as access to data.

Dutch developments

On 13 October 2021, the Dutch Minister of Finance published a report on the progress of the implementation of its national Fintech Action Plan. Key items highlighted in this Action Plan include:

- the development of legislation targeting automatic advice;
- increasing the attention for appropriate fees for new entrants (including fintech start-ups); and
- the statement that Dutch fintech companies should not be subject to stricter requirements than necessary.

The European Commission published a directive proposal along the lines of the OECD Pillar 2 proposal. Adoption of the directive proposal requires a unanimous decision from all EU member states. Directive (EU) 2022/2523 (Pillar 2 Directive) was published in the Official Journal of the European Union on 22 December 2022. Currently, it is intended that EU member states need to implement the Pillar 2 Directive into their national laws by 31 December 2023.

Read this article on Lexology

On 24 October 2022, the Dutch legislator published a draft legislative proposal for the implementation of the Pillar 2 Directive and will prepare a final legislative proposal to be submitted to the Dutch parliament.

Jeroen Bos	jeroen.bos@simmons-simmons.com
Koen van Leeuwen	koen.vanleeuwen@simmons-simmons.com
Marise Kok	marise.kok@simmons-simmons.com

Claude Debussylaan 247, Amsterdam 1082 MC, Netherlands
Tel: +31 20 722 2500
www.simmons-simmons.com

Read more from this firm on Lexology

Read this article on Lexology

New Zealand

Derek Roth-Biester and Megan Pearce

Anderson Lloyd

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 425

General innovation climate 425
Government and regulatory support 426

FINANCIAL REGULATION 426

Regulatory bodies 426
Regulated activities 426
Consumer lending 427
Secondary market loan trading 428
Collective investment schemes 428
Alternative investment funds 428
Peer-to-peer and marketplace lending 429
Crowdfunding 429
Invoice trading 429
Payment services 429
Open banking 430
Robo-advice 430
Insurance products 431
Credit references 431

CROSS-BORDER REGULATION 431

Passporting 431
Requirement for a local presence 432

SALES AND MARKETING 432

Restrictions 432

CRYPTOASSETS AND TOKENS 433

Distributed ledger technology 433
Cryptoassets 433
Token issuance 433

ARTIFICIAL INTELLIGENCE 434

Artificial intelligence 434

CHANGE OF CONTROL 434

Notification and consent 434

Read this article on Lexology

FINANCIAL CRIME 435
Anti-bribery and anti-money laundering procedures 435
Guidance 435

DATA PROTECTION AND CYBERSECURITY 435
Data protection 435
Cybersecurity 436

OUTSOURCING AND CLOUD COMPUTING 436
Outsourcing 436
Cloud computing 436

INTELLECTUAL PROPERTY RIGHTS 437
IP protection for software 437
IP developed by employees and contractors 437
Joint ownership 437
Trade secrets 438
Branding 438
Remedies for infringement of IP 438

COMPETITION 439
Sector-specific issues 439

TAX 439
Incentives 439
Increased tax burden 439

IMMIGRATION 440
Sector-specific schemes 440

UPDATE AND TRENDS 440
Current developments 440

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Fintech in New Zealand is in a very healthy state, driven largely by New Zealand's strong start-up ecosystem, broad base of industry participants and a push from both government and industry to develop a stronger technology export sector in New Zealand. The industry association FinTechNZ acts as a focal point for the fintech community in New Zealand, connecting banks, insurers and managers with investors, innovators and regulators and promoting New Zealand fintech to the world. This promotion is made easier because of New Zealand's excellent international reputation for being a good place to do business, a strong financial system, low corruption and open and approachable regulators.

Read this article on Lexology

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Government departments such as the Ministry of Business and Innovation (MBIE) and regulators such as the Financial Markets Authority (FMA) have demonstrated their strong support of New Zealand fintech, through pro-active engagement with industry participants and with associations such as FinTechNZ and its FinTech Regulatory Roundtable. The Reserve Bank of New Zealand (Reserve Bank), while striking a note of caution on fintech, has nevertheless recognised the efficiencies that it might bring to New Zealand banking and payments systems. Perhaps in recognition of the growth in innovation in this sector, a handful of regulators and government departments, led by the FMA and including MBIE, the Reserve Bank, the Treasury and the Commerce Commission (New Zealand's competition law authority), together formed the Council of Financial Regulators in 2021 to ensure consistent cooperation and assistance between them. In the fintech arena, this has resulted in the creation of the FinTech forum, an online portal through which fintech innovators can seek regulatory guidance. This means of engagement with the fintech community is an example of the well-deserved reputation that the New Zealand regulators have for being open and approachable to new entrants and new products. So while the regulators have stopped short of creating the sort of regulatory sandboxes seen in other jurisdictions, fintech companies are encouraged to engage with the regulators (and with their professional advisers) early on to inform their thinking about potential routes through the regulatory environment.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

There are a number of regulators, depending on the type of products and services being offered. The Financial Markets Authority (FMA) is the securities regulator, which supervises offers of financial products in New Zealand and is responsible for licensing the provision of certain financial services and the enforcement of certain prudential and fair dealing standards. The Reserve Bank is responsible for the supervision and prudential regulation of banks, non-bank deposit takers and insurers as well as generally maintaining the robustness of New Zealand's financial system. Other regulators include the Department of Internal Affairs (anti-money laundering) and the Commerce Commission.

Regulated activities

4 Which activities trigger a licensing requirement in your jurisdiction?

Under the Financial Markets Conduct Act 2013 (FMCA) and subsidiary regulations, if you provide to retail investors any financial advice, crowdfunding services, robo-advice, discretionary investment management services or peer-to-peer (P2P) lending services, or if you operate a managed investment scheme for, issue derivatives (such as contract for differences and forex futures) to or take deposits from retail investors, you will need to be licensed

Read this article on Lexology

by the FMA. Further, any person who carries on 'insurance business' in New Zealand must be licensed by the Reserve Bank. The term 'retail' generally refers to members of the public. Services provided to 'wholesale' investors (of which there are many categories but is the New Zealand equivalent of 'accredited' or 'sophisticated' investors in other jurisdictions) conversely do not require licensing.

In relation to advising on investments, the FMCA's new financial advice regime came fully into force with effect from 17 March 2023. All financial advice providers (FAPs) must hold or operate under a full licence from the FMA if they wish to provide regulated financial advice to retail clients. FAPs can either be an individual or other business entity such as a company. The three classes of FAP licences are Class 1 (sole adviser businesses), Class 2 (businesses that engage more than one adviser) and Class 3 (large organisations that engage 'nominated representatives' among their staff). A nominated representative is an individual engaged by a licensed FAP to give regulated financial advice (which advice must be limited in nature and scope) on their behalf and who does not need their own licence. FAPs, advisers and nominated representatives face a number of compliance obligations under the regime, including adherence to the Code of professional conduct for financial advice services.

Last, there is a separate requirement for any business that provides 'financial services' (whether in New Zealand or from New Zealand to other countries) as required by the Financial Service Providers (Registration and Dispute Resolution) Act 2008 (FSP(RDR)A) to be registered on the Financial Services Provider Register (FSPR).

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Consumer lending is regulated primarily under the Credit Contracts and Consumer Finance Act 2003 (CCCFA), which applies to a range of transactions where money is loaned for personal use such as consumer credit contracts, consumer leases and buy-back transactions. Among other things, the CCCFA and its subsidiary regulations provide general rules for credit contracts and require those to whom the CCCFA applies to adhere to certain 'lender responsibility principles', including by:

- acting responsibly when advertising credit or finance as well as before and after providing consumer credit or finance and taking a relevant guarantee; and
- complying with specific lender responsibilities such as disclosing certain information to borrowers.

The separate Responsible Lending Code elaborates on these principles and provides guidance both on how to comply with them as well as on the information lenders should provide to borrowers before and during the loan term.

The Ministry of Business and Innovation (MBIE) conducted a lengthy review into New Zealand's consumer credit sector and brought in extensive changes to the CCCFA and the Responsible Lending Code in December 2021. The intent was to ease consumer access to credit while maintaining a strong level of consumer protection. Under the new regulations, lenders were required to make certain types of inquiries before agreeing to lend money to a borrower, or before agreeing to provide further credit under an existing loan, including as to

the suitability of the credit product for that consumer and to assess the borrower's income and expenses to be satisfied that the repayments are not likely to cause substantial hardship to the borrower. These changes were initially somewhat controversial, as they were interpreted as requiring lenders to trawl through applicants' bank statements and make possibly invasive enquiries into their lifestyle choices. However, many of these changes were softened by further changes to the CCCFA and the Responsible Lending Code in July 2022 and, most recently, May 2023.

One very popular (until recently) form of consumer finance in New Zealand, buy now, pay later (BNPL), is not as of writing regulated under the CCCFA. However, the MBIE has clearly stated its intention to regulate the BNPL sector and invited submissions on an exposure draft of regulations, entitled the Credit Contracts and Consumer Finance (Buy Now Pay Later) Amendment Regulations 2022, which submissions closed on 10 March 2023. Under these new regulations (which are expected to come into force in 2023), most of the requirements of the CCCFA will apply to BNPL as a 'consumer credit contract' just like credit cards or personal loans. However, smaller amounts of BNPL credit below a dollar threshold (tentatively set at NZ$600) will be exempt from the CCCFA requirement to assess affordability.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

There are no specific restrictions on trading loans, other than in relation to P2P lending. Traders of lending books would need to ensure they contractually have the right to assign the loans and would need to comply with applicable data privacy obligations. P2P lending markets must be licensed providers of a P2P lending service.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Such schemes, in which money from a number of investors is pooled together and those investors are reliant on the investment expertise of the scheme manager, are regulated chiefly as 'managed investment schemes'. The FMCA's definition of these schemes is broad enough to capture most open- and closed-ended collective investment schemes and those involving participatory securities. Fintech companies providing P2P lending or crowdfunding platforms would not be regulated as a managed investment scheme, but instead would be regulated under the relevant licensing regimes for those platforms.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Yes, managed investment scheme managers are required both to register on the FSPR as a provider of financial services and (where they will make a regulated offer to retail investors) to be licensed by the FMA. Managers need to meet and maintain certain minimum

standards (including fitness and propriety of directors and senior managers) and have obligations relating to financial reporting, fair dealing and anti-money laundering.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

P2P lending is regulated by the FMA as a financial market service under the FMCA and anyone who wishes to operate such a market must be licensed as a provider of P2P lending services. Borrowers who use a licensed service are exempted from the requirement to issue a product disclosure statement (which they would otherwise be required to do, as it would be seen as the issue of a debt security to the public). Licensed P2P platforms, in addition to meeting certain minimum standards and conditions for their licence, have a number of ongoing obligations, such as notification of certain events to the FMA (as well as providing an annual regulatory return), and obligations relating to financial reporting, fair dealing and anti-money laundering.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

The FMCA regulates equity-based crowdfunding (where companies raise money from retail investors through the issue of shares) as a financial market service. Reward-based crowdfunding is not covered, nor is any fundraising for charitable or philanthropic purposes (as long as donors do not receive shares). Under the FMCA, companies may raise up to NZ$2 million in any 12-month period on a licensed crowdfunding service provider's platform with minimal regulatory hurdles (such as not having to issue a product disclosure statement). Licensed crowdfunding platforms, in addition to meeting certain minimum standards and conditions for their licence, have a number of ongoing obligations, such as notification of certain events to the FMA (as well as providing an annual regulatory return), and obligations relating to financial reporting, fair dealing and anti-money laundering.

Invoice trading

11 Describe any specific regulation of invoice trading in your jurisdiction.

There is no specific regulation of invoice trading, but it will likely constitute a financial service under the FSP(RDR)A (being a creditor under a credit contract) and require the invoice trader to register on the FSPR as a financial services provider under that Act.

Payment services

12 Are payment services regulated in your jurisdiction?

There currently is no specific regulation of payment services along the lines of Directive (EU) 2015/2366 (revised Payment Services Directive) (PSD2), but such services will constitute financial services under the FSP(RDR)A (as it is issuing and managing a means of payment)

and require the payment services provider to register on the FSPR as a financial services provider under that Act.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

Not yet, as the government has so far preferred to allow the industry to take the lead. The implementation of open banking is being spearheaded by Payments NZ (a company formed by a number of retail banks with the support of the Reserve Bank), which launched its API Centre in May 2019. This is a suite of industry-standardised application programming interfaces (APIs) for payment-related services, which is designed to manage a move to greater openness in banking and payments and to create an API-enabled ecosystem in New Zealand. Payments NZ is responsible for the governance of the API Centre but has delegated it to an API Council comprised of banks, non-bank third parties and independent members. The API Council gets recommendations from a business group and a technical group, and also has an independent sub-committee to handle sensitive issues.

Also relevant to the implementation of open banking is the Consumer Data Right (CDR), which would allow data portability. New Zealand's Minister of Commerce and Consumer Affairs released a cabinet paper in late 2022 making recommendations on the implementation of a legislative framework for a sector-by-sector rollout of a new CDR. The legislation would introduce basic obligations for those operating within the designated sectors and allow consumers to require data holders (such as banks, utilities and healthcare providers) to securely share their data with trusted third parties. The New Zealand banking sector will be the first to implement a CDR, the details of which will be contained in an exposure draft of a data-sharing bill, which is expected to be released for industry feedback before the end of 2023. The cabinet paper suggests that the bill will provide, among other things, for tiered accreditation of data recipients and that penalties for breach of the CDR will be ranked according to their severity, with criminal penalties applying to deliberate or reckless behaviour.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

New Zealand has no specific regulation of robo-adviser. Since the new financial advice provider regime fully came into force in March 2023, the new rules treat advice given by an online digital assistant as being subject to the same rules as advice delivered in person.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Fintech companies that carry on 'insurance business' in New Zealand are subject to the supervision of the Reserve Bank and must be licensed. Whether or not this applies to an insurtech entity will depend on its business activities – under section 8(1) of the Insurance (Prudential Supervision) Act 2010 (IPSA)) it will be held to be carrying on insurance business if it acts as an insurer either within or outside of New Zealand or is otherwise liable as an insurer under a contract of insurance to a New Zealand policyholder. Regulation takes the form of a risk-based supervisory regime established under IPSA, requiring the licensee to meet certain criteria relating to governance, the fitness and propriety of their officers and managers, capital adequacy and liquidity.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Credit reporting has implications under the Privacy Act 2020 (Privacy Act), New Zealand's principal data privacy legislation. In December 2020, after public consultation, the Office of the Privacy Commissioner (OPC) overhauled the Credit Reporting Privacy Code, ostensibly to align the code with the Privacy Act that was being revised at the same time. The code applies specific privacy rules to credit reporters who sell personal credit information. The intent behind this Code is broadly to grant individuals enhanced rights in relation to the use of their personal credit information by these credit reporting agencies. These rights include, among others, imposing time limits on keeping and reporting information, limiting the use of that information to defined circumstances (and in any event requiring consent in most situations), entitling individuals to a free credit score (if the credit reporter has a practice of releasing such scores to subscribers), requiring access to credit information within 10 working days and giving reporters the right to charge for expedited access requests (namely, within three working days), entitling individuals to apply to suppress credit information if they think they have been a victim of fraud and entitling individuals to dispute inaccurate information. Individuals can also complain to the OPC if they think the code has been breached.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

Overseas issuers of financial products wishing to extend the offer into New Zealand will need to do so under an official recognition scheme or under an exemption from the Financial Markets Authority (FMA). To date, there are two such schemes in place, namely:

the Trans-Tasman Mutual Recognition Scheme with Australia, which allows an Australian issuer to extend its offers into New Zealand provided they comply with Australian laws and certain reporting and filing obligations in New Zealand; and

the Asia Region Funds Passport or ARFP, under which a managed fund in the participating countries (Australia, Japan, South Korea and Thailand) may extend the offer to New Zealand provided they:

- register in their home jurisdiction as a passport fund;
- apply to the FMA for authorisation; and
- comply with certain initial and ongoing requirements (including registering on the Financial Services Provider Register, joining a dispute resolution scheme and appointing an agent for service in New Zealand).

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

Any fintech company that provides financial services into New Zealand from overseas is required to register on the Financial Services Provider Register. If its activities in New Zealand constituted 'carrying on business' within the meaning of section 332 of the Companies Act 1993, then it would be required to register with New Zealand's Registrar of Companies as an 'overseas company' (effectively a New Zealand branch of the foreign company). Registration imposes obligations on the company to submit annual financial statements to the Companies Office and may bring it within the remit of New Zealand's anti-money laundering laws.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Part 2 of the Financial Markets Conduct Act 2013 contains a number of fair dealing requirements that will apply to such sales and marketing. Financial service providers must not engage in misleading conduct or make any false, deceptive or unsubstantiated statements about the financial product or service, irrespective of the type of investor they are offering to, or where they are located. Further, New Zealand's Fair Trading Act 1986 (FTA) also prohibits misleading and deceptive conduct in trade and applies to the trading of assets, commodities and other goods and services. Obligations under the FTA are enforced by the Commerce Commission. There are other general consumer laws that may be relevant that prohibit fraudulent conduct such as obtaining money by deception.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

Not currently, although in its November 2022 paper 'The future of business for Aotearoa New Zealand', the Ministry of Business and Innovation consulted on blockchain as one of two trends that will affect future business, and influence productivity and well-being, in New Zealand. The paper identifies that blockchain technology has its benefits and challenges and that robust regulatory development and governance could cause more widespread adoption of the technology, driving innovation in web3, decentralised finance and alternative business structures such as decentralised autonomous organisations. We expect further developments in this space.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

To date, there are no specific rules or regulations applying to the promotion or use of such cryptoassets. The Financial Markets Authority (FMA) has issued guidance on cryptocurrencies and takes the view that any provision of a financial service relating to cryptocurrencies in New Zealand will require compliance with the 'fair dealing' requirements under the Financial Markets Conduct Act 2013 (FMCA) and (potentially) with obligations under the Financial Service Providers (Registration and Dispute Resolution) Act 2008 (FSP(RDR)A) and the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. The guidance states that wallet providers who store cryptocurrency or money on behalf of others, or who facilitate exchanges between cryptocurrencies or between fiat and crypto, will be operating a value transfer service. This is a type of financial service within the meaning of the FSP(RDR)A and requires the provider to register under that Act. Further, if you hold money for depositors you may be offering debt securities (which are financial products regulated under the FMCA), although if those funds are held in trust the wallets may not be debt securities.

Given the extensive public consultations done by the New Zealand government in 2022 around cryptocurrencies generally and the future of money in the context of the possible introduction of a central bank digital currency, we expect this area to develop rapidly going forward.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

There are currently no sector-specific rules or regulations applying to such issuances of tokens. The FMA's commentary to date indicates that it considers the existing regulatory framework contained within the FMCA and subsidiary regulations to be sufficiently

technology-neutral to accommodate these new types of capital raises. The FMA also indicates that the specific characteristics and economic substance of an ICO will determine if it is regulated as a financial product (and, if so, how) and recommends engagement during the development phase of any ICO to discuss the regulatory implications.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

With the arrival of large language models such as ChatGPT, much public and academic debate in recent months has been focused on the impact of artificial intelligence (AI) on New Zealand society, whether or not it should be regulated and, if so, how. In the meantime, there is no specific regulation of AI in New Zealand. Based on comments from the Department of Internal Affairs and other government departments, it is anticipated that Parliament will look to address the use of AI and the use of algorithms in automated decision-making processes by amending existing regulations or legislation on a case-by-case basis, possibly through cross-border efforts with bodies in other jurisdictions such as the OECD AI Policy Observatory.

In relation to robo-advice, any applicant for a financial advice provider that proposes to use a robo-advice tool with its clients will need to describe their digital advice service as part of their application, including any use of artificial intelligence, so that the FMA can assess the service against certain minimum standards around functionality and cyber-resilience.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

A regulated business holding a market service licence issued under the Financial Markets Conduct Act 2013 (FMCA) must notify and report to the Financial Markets Authority (FMA) on the occurrence of 'a material change in circumstances'. This is defined under the FMCA as including any change in the licensee's directors and senior managers or the fulfilment of the eligibility criteria in respect of which the licence was originally granted. Holders of a market service licence must report to the FMA as soon as is practical if the relevant licensee proposes to (among other things):

- change its legal structure;
- enter into any major transaction; or
- enter into a transaction that has the effect of a person obtaining or losing control of the licensee.

On receipt of such reporting, the FMA may suspend, vary or revoke the licensee's market services licence if it considers that, in light of the relevant change, the licensee can no longer meet its licence conditions or any of the minimum criteria in respect of which the original licence was granted.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Yes, if the fintech company carries on one of the many specified activities (including issuing or managing means of payment such as electronic money), which would bring it within the definition of a 'financial institution' under New Zealand's Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AMLCFTA). If it is a financial institution, the fintech company has certain obligations under the AMLCFTA, including conducting a review and assessment of the risk of money laundering specific to its business, implementing a compliance programme, undertaking due diligence on its customers (which could be simplified, standard or enhanced), monitoring transactions and filing suspicious activity reports.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

Not specifically for fintech companies. However, the three supervisors (the Department of Internal Affairs, the Financial Markets Authority and the RBNZ) to whom the AMLCFTA gives responsibility for providing industry guidance have already given general guidance on a number of anti-money laundering topics, including risk assessment, enhanced customer due diligence, beneficial ownership and suspicious activity reporting. Other guidelines published by the New Zealand Police Financial Intelligence Unit may also be relevant.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

Under the Privacy Act 2020, agencies may only disclose personally identifiable information (PII) to an overseas person if the individual concerned authorised the disclosure, the overseas person was a prescribed country or the agency believed on reasonable grounds that the overseas person was required to protect the PII in a manner comparable to the required by the agency under New Zealand law. The Privacy Bill would also provide that the proposed restriction against disclosure of PII to overseas persons should not apply to transfers to cloud storage providers or other overseas processors.

Read this article on Lexology

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

The Crimes Act 1961 provides for a number of cybersecurity regulations that apply to all businesses operating in New Zealand. These include the criminal offences of accessing a computer system for a dishonest purpose or without authorisation, damaging or interfering with a computer system, making, selling, distributing or possessing software for committing a crime and using an interception device. Further, a 2019 report from the Financial Markets Authority contained guidance for regulated entities, recommending that market participants make use of a recognised cybersecurity framework to assist in planning, prioritising and managing their cyber-resilience.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

The Reserve Bank of New Zealand has published an outsourcing policy (last revised in September 2017), which requires large banks (namely, those incorporated as a company in New Zealand with net liabilities exceeding NZ$10 billion) to comply with the policy as a condition of their registration. The objective is to ensure the outsourcing does not compromise the bank's ability to be effectively administered and operated, to facilitate the carrying on of basic banking services by the new owner of all or part of the bank and to address the impact that the failure of an outsourced service provider may have on the bank's ability to carry on all or part of the business of the bank. The Financial Markets Authority (FMA) also has certain rules around outsourcing, for example by requiring certain licensees to ensure their outsourced functions are adequate, effective and comply with their licence obligations.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

Outsourcing arrangements that implement cloud computing would need to comply with the RNBZ's policy and any requirements imposed by the FMA. Cyber risk generally (such as that arising from the use of cloud computing) was one of the issues arising from fintech that was identified by the Financial Stability Board as meriting closer attention. The FMA has also published guidance on cyber-resilience in FMA-regulated financial services, among other things strongly encouraging market participants to use a recognised cybersecurity framework to assist with planning, prioritising and managing their cyber-resilience.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Software is principally protected by New Zealand's copyright laws. Under the Copyright Act 1994, a computer program is a 'literary work' and protected as such upon creation. Subject to special rules for authors who are employees or contractors, the person who is the author of the work is the first owner of the copyright in that work and may freely licence or assign that copyright. The duration of copyright protection is 50 years from the end of the calendar year in which the author dies.

Under the Patents Act 2013, computer programs as such are not patentable in New Zealand. However, if a claim in an application implements software within the invention then it may be patentable. The issue will hinge largely on whether the actual contribution made to the invention lies solely in it being a computer program – if so, then no patent can be granted.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Under section 21(2) of the Copyright Act, if an employee creates any works in the course of their employment, then their employer is the first owner of the copyright in that work. A similar but narrower provision is contained in section 21(3) in relation to contractors and consultants. This section provides that if a person commissions and pays or agrees to pay for one of the artistic works specified in that section (namely, a computer program, photograph, painting, drawing, diagram, map, chart, plan, engraving, model, sculpture, film or sound recording) and the work is made in pursuance of that commission, then the commissioner is the first owner of the copyright in that work. For any other kind of work capable of copyright protection, a provision regarding IP ownership would need to be made in the applicable consulting agreement.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

This will depend on the type of intellectual property in question. For example, under the Copyright Act, an exclusive licence of a copyrighted work is required to be in writing signed by or on behalf of all joint owners, but otherwise, the joint owners are free to use, licence, charge or assign their rights in that work. Under section 24 of the Patents Act 2013, absent any agreement to the contrary, co-owners of patents are each entitled to exercise the exclusive rights given by the patent for their own benefit without accounting to the others, but cannot assign or grant a licence of the patent without the consent of all co-owners.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Trade secrets are protected not by statute but under common law principles of breach of confidence and the laws of contract (including under contracts of employment). Owners of trade secrets do not need to, and indeed cannot, register their trade secrets for them to be protected – instead, they would bring an action for breach of contract (where the infringement of the trade secret constituted a breach of that contract) and/or for the tort of breach of confidence. The courts recognise an obligation on a person who unlawfully receives confidential information not to take unfair advantage of it and are able to grant injunctions to give effect to these obligations.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

New Zealand's Trade Marks Act 2002 provides for a system of registration of trademarks. These are not limited to just words or logos, but can include symbols, phrases, shapes or sounds. There is no requirement to register a mark – indeed unregistered marks can be protected using the common law tort of passing off. However, registration gives the owner the exclusive right to use the mark in New Zealand in the class in which it is registered, as well as giving it a defence against infringement claims. Fintech companies looking not to infringe an existing brand can do an online search of the trade mark register maintained by the Intellectual Property Office of New Zealand (IPONZ) either by themselves, or ask IPONZ to conduct a clearance search before registering their own trade mark. Domain name searches and searches of the Companies Office register can also be done to determine if the desired domain and company name are available for registration.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

The usual civil remedies are available including monetary damages, summary judgment, injunctive relief (including ex parte), specific performance (such as delivery up of infringing articles as well as corrective advertising) and civil search and seizure orders. The rights holder may also plead misleading and deceptive conduct in trade in breach of the Fair Trading Act 1986. The Copyright Act also provides for criminal liability for infringement of copyright works for commercial gain.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

There is no fintech-specific competition regulation in New Zealand. However, one has to assume that if fintech and open banking take off in New Zealand it will have competition law implications that will be of interest to New Zealand's competition regulator, the Commerce Commission. Competition law in New Zealand is governed by the Commerce Act 1986 and its subsidiary regulations, and is already being applied by the Commerce Commission to regulate behaviour in the sector.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

Fintech businesses can take advantage of the research and development (R&D) tax incentive. This is a tax credit equal to 15 per cent of eligible R&D spending up to NZ$120 million. To be eligible, the business has to spend NZ$50,000 or more per year on 'eligible R&D', although spending under this level may still be eligible if the R&D is done through an approved research provider on your behalf. The eligible R&D must be carried out in New Zealand, subject to a 10 per cent cap on total eligible R&D spending being carried out outside of New Zealand.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

In February 2019, the coalition government outlined a draft implementation of a new 'digital services tax' intended to capture what is thought to be lost revenue from online platforms, social networks and content-sharing platforms. One of the suggestions was a flat 3 per cent tax on the gross turnover of such digital businesses, but the final form will only become uncertain if or when the tax comes into force.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

Immigration New Zealand maintains lists of skill shortages and there are many technology-related jobs on those lists. Depending on the particular role and your age, qualifications and post-graduate work experience, immigrants may be able to enter New Zealand on a Skilled Migrant Category Resident Visa (which is points-based and allows an indefinite length of stay) or under the Long Term Skill Shortage List Work Visa (which is a temporary work to residence visa valid for up to 30 months and requires that the applicant have an existing offer of one of the jobs on the list). If the job is not on the list, then there may still be other visas available.

UPDATE AND TRENDS

Current developments

41 Are there any other current developments or emerging trends to note?

The legislative and regulatory environment in New Zealand is constantly changing through initiatives such as the future of money and central bank digital currency consultation and design, the Digital Identity Programme and Consumer Data Right. We expect all of these developments and others to have flow-on implications for fintech in New Zealand.

anderson lloyd.

Derek Roth-Biester derek.roth-biester@al.nz
Megan Pearce megan.pearce@al.nz

Level 2, 13 Camp Street, Queenstown 9300, New Zealand
Tel: +64 3 450 0700
www.al.nz

Read more from this firm on Lexology

Read this article on Lexology

Nigeria

Ugochukwu Obi, Tare Olorogun, Omolade Afonja, Adesola Baruwa and Anthony Obidike

Perchstone & Graeys

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 442
General innovation climate 442
Government and regulatory support 443

FINANCIAL REGULATION 444
Regulatory bodies 444
Regulated activities 444
Consumer lending 445
Secondary market loan trading 445
Collective investment schemes 445
Alternative investment funds 446
Peer-to-peer and marketplace lending 446
Crowdfunding 446
Invoice trading 446
Payment services 447
Open banking 447
Robo-advice 447
Insurance products 448
Credit references 448

CROSS-BORDER REGULATION 448
Passporting 448
Requirement for a local presence 449

SALES AND MARKETING 449
Restrictions 449

CRYPTOASSETS AND TOKENS 450
Distributed ledger technology 450
Cryptoassets 450
Token issuance 450

ARTIFICIAL INTELLIGENCE 451
Artificial intelligence 451

CHANGE OF CONTROL 451
Notification and consent 451

FINANCIAL CRIME 451

Read this article on Lexology

Anti-bribery and anti-money laundering procedures 451
Guidance 452

DATA PROTECTION AND CYBERSECURITY 452
Data protection 452
Cybersecurity 452

OUTSOURCING AND CLOUD COMPUTING 453
Outsourcing 453
Cloud computing 453

INTELLECTUAL PROPERTY RIGHTS 453
IP protection for software 453
IP developed by employees and contractors 453
Joint ownership 454
Trade secrets 454
Branding 454
Remedies for infringement of IP 455

COMPETITION 455
Sector-specific issues 455

TAX 455
Incentives 455
Increased tax burden 456

IMMIGRATION 456
Sector-specific schemes 456

UPDATE AND TRENDS 456
Current developments 456

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Fintech has disrupted the Nigerian financial services industry. Innovators in the fintech space are now developing disruptive value propositions across the financial services value chain to address the needs of consumers in different areas such as payment and remittances, micro-investment and savings, wealth management, lending, and buy now, pay later services, etc. Nigeria now has several mobile applications developed by fintech startups that allow users to send and receive money via their mobile phones. There has been a noticeable increase in mobile lending products targeting small and medium-sized enterprises and retail consumers. These products allow users to apply for quick, unsecured, and short-term loans, leveraging advanced technologies such as machine learning for credit risk analysis and assessment. To remain competitive and relevant in the financial space, the traditional banks are also digitising their own offerings and services as well, partnering with the fintech startups, or developing their own solutions. For example, in 2019, a leading commercial

Read this article on Lexology

bank in Nigeria, Guaranty Trust Bank, launched a data centre and has developed interactive and intelligent bots to deliver faster and more personalised banking services.

The key drivers of fintech innovation in Nigeria are a combination of several factors that include the country's youthful population, increasing smartphone and internet penetration, and a focused regulatory drive to increase financial inclusion and entrench a cashless payment environment. However, fintech adoption is highest among middle-class and affluent customers who live in urban areas. To date, mobile payment channels have emerged as the most preferred and convenient way of conducting financial transactions in Nigeria, made possible through fintech innovation.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

The growth of the fintech industry is largely facilitated and aided by the federal government's financial inclusion and digital economic policies. In the implementation of these policies, several regulations were issued by the relevant government agencies or regulators to promote fintech innovations and to make the industry safer for consumers. For example, the Central Bank of Nigeria (CBN) published the Framework for Regulatory Sandbox Operations in January 2021 to regulate the entry of new tech products by providing a controlled environment for their trial; thus, making it safer for consumers. Specifically, the framework will benefit stakeholders in the technology and financial sectors as it encourages innovation to improve the delivery of payment services and is suited for products and services not covered by existing legislation. There is also the Open-Banking Regulation, issued by the CBN in May 2021, that encourages the sharing of financial data through an application programming interface by setting out the requirements for the secured sharing of such information. This is beneficial to technology companies that rely on financial data that are ordinarily within the exclusive possession of traditional banks. Notably, open banking will enable the lenders to have an accurate assessment of the financial status of the borrowers thus allowing them to provide more profitable lending terms. In 2022, the Securities and Exchange Commission issued the Rules on the Issuance, Offering Platform, and Custody of Digital Assets, which now seeks to protect consumers desirous of investing in digital tokens securities by requiring registration of such securities. A major advantage of the rules is that it allays the fear of investors who seek to provide capital for the operation of a business through digital asset offerings by providing documentation requirements, due diligence, registration, and the limit of funds to be raised. Also in the same year, the Nigeria Startup Act was introduced to harness the potential of our digital economy through co-created regulations. The Act is aimed at ensuring that Nigerian laws and regulations are clear, planned, and work for the tech ecosystem. Nigeria also has the CBN Guidelines on Payment Service Banks for Telcos to bridge the gap in financial inclusion and deepen banking services in Nigeria. While traditional banks will usually require stringent know-your-customer and compliance requirements in the offering of financial services, the Guidelines seek to ensure that payment service banks can provide basic banking and financial services to unbanked in the rural areas or underserved areas.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

Bodies regulating Nigeria's fintech comprise:

- the CBN;
- the Securities and Exchange Commission (SEC);
- the Corporate Affairs Commission (CAC);
- the National Insurance Commission;
- the Nigerian Communications Commission;
- the Nigerian Deposit Insurance Commission;
- the Nigerian Information Technology Development Agency;
- the Nigerian Data Protection Bureau;
- the Federal Competition and Consumer Protection Commission; and
- the Standard Organisation of Nigeria.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

General licensing:

- operating a corporate entity in Nigeria: incorporation of the company at the CAC;
- foreign Investors to operate a business in Nigeria: obtain a business permit from the Federal Ministry of Interior;
- providing financial services: licensing with the CBN; and
- dealing in securities: registration with SEC.

Specific licensing:

- operating a crowdfunding platform: registration with SEC;
- issuing digital assets as securities to raise funds: registration with SEC;
- operating a digital asset offering platform: registration with SEC;
- operating a digital asset exchange platform: registration with SEC;
- operating a digital asset custodian: registration with SEC;
- wealth or portfolio management: registration with SEC;
- operating a financing company (such as consumer loans, fund management, asset financing): registration with the CBN;
- operating a payment service bank: registration with the CBN; and
- capital importation: obtaining a certificate of capital importation from the CBN.

Read this article on Lexology

Consumer lending

5 Is consumer lending regulated in your jurisdiction?

Unlike commercial lending, consumer lending is still developing in Nigeria. The CBN's Revised Guidelines for Finance Companies in Nigeria, of 2014, provides for the registration of finance companies, including companies that provide consumer loans. Most of the time, consumers turn to Microfinance Banks (MFBs) to obtain microloans for personal or household use. The MFBs are regulated by the CBN's Revised Regulatory and Supervisory Guidelines for Microfinance Banks. At state level, the moneylending laws of various states generally regulate moneylending in Nigeria. Under the laws, a company or individual who intends to lend money at an interest rate in Nigeria must obtain a moneylender licence. Section 5 of the Money Lenders Law of Lagos State requires an entity to be licensed before the commencement and operation of a moneylending business.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

No. Debt instruments can be traded in the secondary market, provided they meet the basic criteria for trading in the secondary market like the Financial Market Dealers Quotations Group Plc (FMDQ). FMDQ Group Plc (FMDQ Group), which commenced as an over-the-counter market is a Securities and Exchange Commission-registered capital market holding company warehousing five wholly owned subsidiaries including FMDQ Securities Exchange Limited, FMDQ Clear Limited, FMDQ Depository Limited, FMDQ Private Markets Limited and IQX Consult Limited.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Collective investment schemes in Nigeria are regulated by:

- the Securities and Exchange Commission 2013 Rules (the Rules);
- the SEC New Rules and Amendments to the Rules; and
- the Regulations of the Commission, dated 21 January 2021.

These rules protect investors who wish to pool their funds and cover activities or products such as fund management products, collective investment schemes and crowdfunding (and crowdfunding platforms). Fintech companies that offer investment services or crowdfunding platforms fall within this scope and are required to obtain an SEC licence before seeking funds from investors or engaging in any capital market operations in Nigeria.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Yes, managers of alternative investment funds such as venture capital managers and private equity funds are regulated by the SEC. An example of such regulation are the Rules on Private Equity Funds, Rule 249D of 28 February 2013. Venture capital managers are required to be registered with the SEC while the private equity fund is subject to authorisation and registration by the SEC.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Peer-to-peer lending is still developing in Nigeria. Generally, the Banks and Other Financial Institutions Act 2020 (BOFIA) regulates financial activities in Nigeria. Section 3 of BOFIA requires any entity that would provide financial services must have a banking licence. Also, any entity that intends to provide lending services must, in addition to obtaining the relevant CBN licence, obtain a moneylending licence in accordance with the moneylending laws of the various states. Digital lenders must also comply with Nigeria's Data Protection Regulation 2019.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

The SEC New Rules and Amendments to the Rules and Regulations of the Commission, dated 21 August 2021, specifically regulate crowdfunding in Nigeria. Any entity seeking to raise funds through a crowdfunding portal must, among other requirements, be a micro, small or medium enterprise incorporated in Nigeria. The maximum amount that can be raised within 12 months depends on whether the company is classified as a micro (50 million naira), small (70 million naira), or medium enterprise (100 million naira.) The Rules provide that a crowdfunding portal shall be operated only by an entity registered as a crowdfunding intermediary.

Invoice trading

11 Describe any specific regulation of invoice trading in your jurisdiction.

There is generally no specific regulation for invoice trading in Nigeria. Generally, the CBN via the Banks and Other Financial Institutions Act 2020, regulates activities such as factoring, financing, debt administration, etc. However, the Factoring Bill is currently being deliberated at the National Assembly.

Payment services

12 Are payment services regulated in your jurisdiction?

BOFIA expressly brings payment services within the regulatory powers of the CBN. Under BOFIA, they are referred to as other financial institutions (OFIs). While BOFIA generally makes provisions for banks and OFIs, specific and more detailed instruments guiding the provision of services as a payment service provider are provided in numerous regulations, circulars, guidelines and frameworks. These include:

- the New License Categorisations for the Nigerian Payment System, dated 9 December 2020 (the License Categorisation);
- the CBN Guidelines on Operation of Electronic Payment Channels in Nigeria 2020; and
- the Supervisory Framework for Payment Service Banks, July 2021.

The License Categorisation categorises payment services in Nigeria into:

- switching and processing;
- mobile money operations;
- payment solutions services (which includes agency banking, payment terminal service providers and payment solutions service providers such as payment gateways or portals); and
- regulatory sandbox.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

Yes. These laws are:

- the CBN Regulatory Framework for Open Banking;
- the CBN Operational Guidelines for Open Banking in Nigeria;
- the Federal Competition and Consumer Protection Act;
- the National Information and Technology Development Act; and
- the CBN Consumer Protection Consumer Framework for Banks and Other Financial Institutions.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

The major regulatory framework for robo-advisory services in Nigeria are the SEC Rules on Robo-Advisory Service in Nigeria, dated 30 August 2021 (the Rules). The SEC, the sole regulator of capital markets in Nigeria introduced the Rules applicable to people who carry out robo-advisory services in Nigeria. By the Rules, a robo-adviser is required to comply,

on an ongoing basis, with all the applicable business conduct requirements set out in the Investment and Securities Act (ISA) and the rules, regulations, notices and guidelines issued pursuant to the ISA. The Rules also provide that robo-advisers shall implement internal policies and procedures to address technology risks.

Other regulatory frameworks that may affect robo-advisers in Nigeria include:

- the SEC Guidelines on Technology Risk Management;
- the SEC Regulation on Anti-money Laundering and Combating the Financing of Terrorism Act 2013;
- the SEC Advertisement Requirements; and
- the Code of Conduct for Employees of Capital Market.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Yes, they do. The National Insurance Commission issued the Insurance Web Aggregators Operational Guidelines (the Guidelines) on 1 February 2022. The Guidelines provide for, and guide the registration, supervision and monitoring of insurance web aggregators in Nigeria.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Yes, there are. The Credit Reporting Act 2017 (CRA) is the primary regulatory framework for credit referencing and credit information services in Nigeria. The CRA provides for the licensing and regulation of credit bureaus and also stipulates the various maintenance and sharing of credit information among other players.

To carry out credit information services as a credit bureau in Nigeria, such person shall obtain a licence from the CBN in accordance with the provisions of the CRA. The CRA also provides that in performing its functions, a credit bureau shall not release or provide information to any credit information user with which it does not have a data exchange agreement unless the written or other authenticated consent of the relevant data subject has been obtained and shown to a credit bureau. The instant provision restricts a credit bureau from providing credit information to any credit-information user with which a credit bureau does not have a data-exchange agreement.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

No. Regulated activities cannot be passported into the Nigerian jurisdiction.

Read this article on Lexology

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

No. By the provisions of the Companies and Allied Matters Act 2020 (CAMA), any person or entity wishing to carry on business in Nigeria must duly register same with the Corporate Affairs Commission unless such person or entity falls within the exemptions in section 80 of CAMA. The exempted entities are:

- foreign companies invited by, or with the approval of, the federal government to execute specified individual projects;
- foreign companies that are in Nigeria for the execution of specified individual loan projects on behalf of a donor country or international organisation;
- foreign government-owned companies engaged in export promotion activities; and
- engineering consultants or technical experts engaged in any individual specialist project under contract with any of the governments in the federation or any of their agencies or with any other body or person, where such contract has been approved by the federal government.

Where such fintech company does not fall within this scope, it must be registered in Nigeria. However, the regulators recognise the need for partnerships with foreign entities for some fintech activities. For example, the Central Bank of Nigeria (CBN) Guidelines on International Money Transfer Service in Nigeria provide that a money transfer operator (MTO) may engage a foreign technical partner to provide global or regional payment or money transfer platform, provided that such MTO obtains a letter of no objection from the CBN. Such a foreign technical partner must, among others, be a registered entity licensed to carry out money transfers in its home country.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

There is generally no restriction on the sale and marketing of financial services in Nigeria. However, the Securities and Exchange Commission (SEC) issued a circular to all capital market operators, restricting them from assisting and facilitating online investment and trading platforms to have direct access to the securities of foreign companies not registered in Nigeria. On 11 May 2022, the SEC also issued the Rules on the Issuance, Offering Platform, and Custody of Digital Assets, which requires that digital assets offering platform and digital assets offered by issuers to the public (to raise funds) be registered with the SEC. Also, it should be noted that the Central Bank of Nigeria (CBN) issued a notice to deposit money banks to refrain from facilitating payment transactions associated with cryptocurrency trading.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

No, there are no regulations governing the use of blockchain technology in Nigeria. However, the Securities and Exchange Commission (SEC) issued the Rules on the Issuance, Offering Platform, and Custody of Digital Assets 2022, which regulate the issuance of digital assets as securities in Nigeria. The Rules regulate the digital asset offering (including initial coin offerings and other distributed ledger technology offers of digital assets) in Nigeria or targeting Nigerians. Also, in May 2023, the Federal Government of Nigeria issued the National Blockchain Policy. The policy seeks to provide a roadmap for Nigeria's adoption and utilisation of blockchain technology. The Policy lays out a comprehensive framework for integrating blockchain technology into different spheres of the economy. It also addresses key issues such as governance, interoperability, security, and regulatory compliance. In addition to these, it offers direction and guidance to stakeholders in both the public and private sectors to ensure the adoption, innovative and responsible use of blockchain technology.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

Yes. The SEC has released new Rules on Issuance, Offering Platforms, and Custody of Digital Assets 2022. Also, the CBN issued a circular to banks prohibiting the processing of crypto-related payment transactions. It should, however, be noted that in 2021, the CBN issued the e-Naira, its central bank digital currency, and the Regulatory Guidelines on the eNaira, dated October 2021.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Yes, the SEC has released new Rules on Issuance, Offering Platforms and Custody of Digital Assets 2022, which regulate the offering of digital assets including initial coin offerings.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

No, there is currently no law relating to artificial intelligence in Nigeria. However, the Securities and Exchange Commission issued the Rules on Robo-Advisory Service in Nigeria, dated 30 August 2021 to regulate people who carry out robo-advisory services in Nigeria.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

The Federal Competition and Consumer Protection Act 2019 (FCCPA) provides for the notification of a merger to the Federal Competition and Consumer Protection Commission (the Commission). The FCCPA provides that a party to a small merger may voluntarily notify the Commission of that merger at any time, while it is mandatory for a party to a large merger to notify the Commission in the prescribed form and manner. Further, the Commission mandates that a proposed merger shall only be implemented upon notification and approval of the FCCPC. The Securities and Exchange Commission's prior approval must also be obtained where any of the merging entities is a public company.

Returns of change in control or ownership of a company must also be filed with the Corporate Affairs Commission.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Yes. The Central Bank of Nigeria (CBN) Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions Regulations 2013 imposes an obligation on all financial institutions, including fintech companies, to have policies on anti-money laundering (AML) and countering the financing of terrorism, as well as appropriate know-your-customer requirements and record keeping. They are mandated to take appropriate steps to identify, assess and understand their money laundering risks for specific customers on their platform and areas of operation. Moreover, they are required to report suspicious fund transfers to the CBN.

Read this article on Lexology

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

The following laws generally govern AML and financial crimes in Nigeria:

- the Advance Fee Fraud and other Fraud Related Offences Act 2006;
- the Banks and Other Financial Institutions Act 2020;
- the CBN Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria Regulations 2013;
- the Corrupt Practices and Other Related Offences Act 2000;
- the Economic and Financial Crime Commission (Establishment) Act 2004;
- the Money Laundering (Prohibition) Act 2011 (as amended);
- the Terrorism Prevention (Freezing of International Terrorist Funds and other Related Matters) Regulations 2013; and
- the Terrorism Prevention Act 2012 (as amended).

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The Nigeria Data Protection Regulation 2019, is the principal regulation and framework for the governance of data protection in Nigeria. The Operational Guidelines for Open Banking in Nigeria 2022 also regulate the sharing of financial data via an application programming interface.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

The Cybercrime (Prohibition, Prevention) Act 2015 is the principal regulation that guides and regulates all cybersecurity or cybercrimes in Nigeria. In specific relation to deposit money banks and payment service providers, the Central Bank of Nigeria also released the Risk-Based Cybersecurity Frameworks and Guidelines for Deposit Money Banks and Payment Service Providers.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

No, there is no general regulatory guidance for the outsourcing of financial services in Nigeria. However, the Rules on Issuance, Offering Platforms and Custody of Digital Assets 2022 provides for (and regulates) the outsourcing of some of the activities of digital asset offering platforms, digital asset custodians and digital asset exchange operators.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

In August 2019, the National Information Technology Development Agency issued the Nigerian Cloud Computing Policy, adopting cloud computing by the Nigerian government. The policy promotes 'cloud first' as a proposition to federal public institutions and small to medium-sized enterprises as an efficient way of acquiring and deploying computing resources for improved quality of digital services.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Intellectual property rights available for the protection of software in Nigeria are copyright and patents, and are governed by the Nigerian Copyrights Act and the Patent and Designs Act, respectively. Generally, no formal application is required to obtain copyright protection; however, an applicant may decide to register formally by an application to the Nigerian Copyrights Commission. In the same vein, a patent can be obtained by an application to the Registrar of Patents and Trade if such software is new, or constitutes an improvement to an existing patented innovation.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Under the Nigerian Copyright Act, unless otherwise stated in a contract of employment, copyright shall belong in the first instance to the author (the employee). However, where a literary work is made by the author in the course of his or her employment by the proprietor

Read this article on Lexology

under a contract of service or apprenticeship for the purpose of publication, the said proprietor shall, in the absence of any agreement to the contrary, be the first owner of copyright in the work in so far as the copyright relates to the publication. In all other respects, the author shall be the first owner of the copyright in the work.

For patents, the Patents and Designs Act vests designs and inventions made in the course of employment in the employer and gives little or no room for separate contracts to state otherwise. However, in practice, the employee (who, most often, is the inventor) would assign his or her rights to the employer to back up the application for the issuance of a patent.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Yes, the Patents and Designs Act places a restriction on joint owners of a licence assigning the same contractual rights to a third party differently. Thus, subject to the contract between parties, joint owners may individually transfer or assign their shares in intellectual property but cannot individually license their share in intellectual property; it must be done jointly. Aside from granting their licence, restrictions are subject to a contract between parties.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Trade secrets are generally protected by non-disclosure agreements binding the parties and preventing them from disclosing sensitive information about their respective companies.

Although trade secrets are not a statutory form of intellectual property rights, they can be used to prevent the unauthorised disclosure of sensitive information. Thus, the most practised way of protecting trade secrets is by signing a non-disclosure agreement. Often, non-disclosure agreements are drafted to bind parties as to the secrecy of certain information they are privileged to know. Other ways of protecting trade secrets include non-compete clauses or agreements and using sophisticated IT security infrastructure.

The courts in Nigeria generally uphold the sacrosanct nature of trade secrets. However, wherein a matter, there is an overriding public interest that, if ignored, will result in a miscarriage of justice, the court will direct that such trade secret should be made public or disclosed in the interest of justice.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

The intellectual property rights available to protect branding in Nigeria are trademarks and copyrights.

Read this article on Lexology

No formal application is required to obtain copyright protection, as such work is automatically protected once it is created. However, aside from copyright, which is protected automatically, other intellectual property can be obtained by an application to the various commissions or registries in charge of each intellectual property right.

To prevent an infringement upon an existing brand, fintech companies must conduct searches at various commissions or registries to ensure that such an intended brand has not been registered.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

The remedies available to individuals or companies whose IP rights have been infringed include an action for IP infringement. The aggrieved party may obtain an order of the court compelling the defendant to account for all profits made from such infringement and remit the same to the aggrieved party, or they may also obtain an order of court enabling them to gain access to the defendant's premises and take possession of the infringed products (*Anton Pillar* injunction). The court with the jurisdiction to hear IP matters in Nigeria is the Federal High Court.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

The fintech space in Nigeria is well-regulated. However, some provisions of relevant regulations may be too stringent for fledging start-ups within the fintech industry. One of these requirements is shareholders 'funds unimpaired by losses' required to be deposited with the Central Bank of Nigeria when applying for specific licences within the payment system industry.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

There are currently no incentives specifically available to fintech companies in Nigeria. However, incentives are generally available to companies in Nigeria. The Finance Act 2019 exempts companies with a turnover of 25 million naira or less from companies' income tax, value added tax and tertiary education tax. Also, companies classified as operating in a pioneer industry or engaged in the production of pioneer products, are exempted from the

payment of companies' income tax for three years. The Venture Capital (Incentives) Act 2004 provides that companies that invest in venture projects may, upon approval, be eligible for capital allowances for up to 30 per cent and exemption from capital gains tax.

The Startup Act 2022 also provides labelled start-ups with some tax incentives such as:

- tax reliefs and incentives granted under the Pioneer Status Incentives;
- exemption from contributions to the Industrial Training Fund; and
- investment tax credit for up to 30 per cent.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

No, there are currently no tax laws in Nigeria that would significantly increase tax or administrative costs for fintech companies. However, by the Companies Income Tax (Significant Economic Presence) Order 2020, non-resident companies (who have a significant economic presence in Nigeria) providing digital services to Nigeria will now be required to pay taxes.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

There are currently no special immigration schemes specific to fintech businesses in Nigeria. Hence, fintech companies that wish to recruit skilled foreign staff must comply with established regulations for such recruitment, by making an application to the Federal Ministry of Interior for the issuance of an expatriate quota with respect to the relevant number of expatriate personnel it intends to employ. In the alternative, the company can also apply for a temporary work visa, which will only be valid for three months.

UPDATE AND TRENDS

Current developments

41 Are there any other current developments or emerging trends to note?

The Securities and Exchange Commission issued the Rules on Issuance, Offering Platforms, and Custody of Digital Assets 2022, which now regulates the issuance of digital assets to the public. The Nigerian Startup Act was signed into law in 2022 and it aims to create an enabling environment to attract and protect investments in the tech startup space. The Business Facilitation Act 2023 was also signed into law to aid the ease of doing business in

Nigeria. In the same vein, the Securitisation Bill and Factoring Bill are currently before the National Assembly.

Ugochukwu Obi	ugochukwuobi@perchstoneandgraeys.com
Tare Olorogun	tareolorogun@perchstoneandgraeys.com
Omolade Afonja	omoladeafonja@perchstoneandgraeys.com
Adesola Baruwa	adesolabaruwa@perchstoneandgraeys.com
Anthony Obidike	anthonyobidike@perchstoneandgraeys.com

1 Perchstone and Graeys Close, Off Remi Olowude, Lagos, Nigeria
Tel: +234 1 761 1051
www.perchstoneandgraeys.com

Read more from this firm on Lexology

Read this article on Lexology

Singapore

Ying Wang and Ashleigh Low
Simmons & Simmons

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 459
General innovation climate 459
Government and regulatory support 460

FINANCIAL REGULATION 461
Regulatory bodies 461
Regulated activities 462
Consumer lending 463
Secondary market loan trading 464
Collective investment schemes 464
Alternative investment funds 465
Peer-to-peer and marketplace lending 465
Crowdfunding 465
Invoice trading 466
Payment services 466
Open banking 467
Robo-advice 468
Insurance products 469
Credit references 469

CROSS-BORDER REGULATION 469
Passporting 469
Requirement for a local presence 470

SALES AND MARKETING 470
Restrictions 470

CRYPTOASSETS AND TOKENS 470
Distributed ledger technology 470
Cryptoassets 471
Token issuance 471

ARTIFICIAL INTELLIGENCE 472
Artificial intelligence 472

CHANGE OF CONTROL 473
Notification and consent 473

Read this article on Lexology

FINANCIAL CRIME 473
Anti-bribery and anti-money laundering procedures 473
Guidance 473

DATA PROTECTION AND CYBERSECURITY 474
Data protection 474
Cybersecurity 474

OUTSOURCING AND CLOUD COMPUTING 475
Outsourcing 475
Cloud computing 476

INTELLECTUAL PROPERTY RIGHTS 476
IP protection for software 476
IP developed by employees and contractors 477
Joint ownership 477
Trade secrets 477
Branding 478
Remedies for infringement of IP 478

COMPETITION 478
Sector-specific issues 478

TAX 479
Incentives 479
Increased tax burden 480

IMMIGRATION 480
Sector-specific schemes 480

UPDATE AND TRENDS 480
Current developments 480

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Singapore provides a conducive fintech ecosystem with supporting regulations, customer demand, strong investments and the potential for high returns. The government considers a vibrant fintech sub-sector key to Singapore's vision for a Smart Financial Centre – a subset of the Smart Nation initiative.

According to a survey by FinTech Global, funding in Singapore's fintech sector reached a total of S$2.4bn in 2022, albeit a 29 per cent decline from 2021. Nevertheless, Singapore saw their most active year for fintech in 2022 with 232 deals raised by Singaporean companies (representing a 12 per cent increase in 2022), which has set a new record for the country.

Based on the Innovation page of the Monetary Authority of Singapore (MAS), there are currently more than 1,000 fintech start-ups operating in Singapore, and there are more

than 40 innovation labs in Singapore. The Singapore FinTech Association, the industry association, has enabled the development of the ecosystem by facilitating collaboration between market participants and stakeholders. There are various grants for start-ups looking to start a business in Singapore.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

MAS is a member of the Global Financial Innovation Network (GFIN), which was formally launched in January 2019 by an international group of financial regulators and related organisations. The GFIN is committed to supporting financial innovation in the interests of consumers and helping innovative firms navigate between countries as they look to scale new ideas. A cross-border testing pilot programme was launched in 2019 to allow firms to simultaneously trial and scale new technologies in multiple jurisdictions, gaining real-time insight into how a product or service might operate in the market.

As of March 2023, MAS had signed 36 fintech cooperation agreements with other countries, including Abu Dhabi, Australia, China, Canada, France, the United Kingdom and the United States, to foster closer cooperation on fintech and to promote innovation in financial services in their respective markets.

MAS released a consultation paper on 14 November 2018 to propose the creation of predefined sandboxes, known as Sandbox Express, to complement the existing FinTech Regulatory Sandbox launched in 2016. The proposed predefined sandboxes would enable firms to embark on experiments more quickly without needing to go through the existing bespoke sandbox application and approval process if the intended activities entail risks that are generally low or could be reasonably contained within the specific predefined sandbox with its predetermined boundaries, expectations and regulatory reliefs. Most recently, MAS has introduced Sandbox Plus, which makes three enhancements:

- expansion of eligibility criteria to include early adopters of technology innovation;
- streamlined application with a financial grant for first movers of technology innovation; and
- participation in the Deal Fridays programme, a platform for deal-making opportunities. Sandbox Plus has been effective as of 1 January 2022.

MAS has encouraged engagement with the industry and has been open to discussing the support it can provide in forms such as financial support, training and mentorship. In 2016, MAS opened a fintech innovation lab, Looking Glass@MAS, to provide a platform for the fintech community to connect, collaborate, and co-create with one another, and MAS also regularly publishes sets of data as application programming interfaces on its website to encourage and facilitate development of innovative solutions.

In 2015, MAS launched the Financial Sector Technology and Innovation (FSTI) scheme to support innovation initiatives in the finance industry. Under the scheme, MAS set aside S$225 million over five years for the development of fintech, to attract financial institutions to establish their research and development and innovation hubs in Singapore, to support

the construction of industry-wide technological infrastructure to deliver innovative integrated services and to catalyse financial institutions to develop creative solutions promoting growth, efficiency and competitiveness. Following overwhelming applications, MAS has supplemented the FSTI scheme with the enhanced FSTI 2.0 scheme by committing an additional S$250 million over three years.

Under FSTI 2.0, MAS will commit S$42 million towards the Regulatory Technology (RegTech) grant scheme and enhancement of the Digital Acceleration Grant (DAG) scheme to accelerate technology adoption in the financial sector. The RegTech grant scheme aims to promote the adoption and integration of technology solutions in the risk management and compliance functions of Singapore-based financial institutions (FIs). Similarly, the Enhanced DAG aims to supplement the existing DAG scheme to be launched in April 2020 to help smaller FIs and fintech firms adopt digital solutions to better cope with the impact of the covid-19 pandemic. In response to the 1,100 applications for the DAG scheme, MAS will commit an additional S$30 million to the DAG scheme. The FSTI 2.0 scheme is valid until March 2023, and MAS plans to provide a third tranche of funding of S$150 million for the next three years with a stronger focus on areas such as AI, analytics, RegTech, Cyber Security and ESG FinTech. More details will be provided by MAS sometime in the first or second quarter of 2023.

MAS, Singapore Fintech Association and AMTD established a S$6 million MAS-SFA-AMTD FinTech Solidarity Grant during the covid-19 period to support Singapore-based fintech companies amid the challenging business climate caused by the covid-19 pandemic. The Grant will help the fintech firms manage their cashflow better, support them in generating new businesses, and provide greater support for fintech firms to pursue growth strategies.

Additionally, MAS has partnered with ASEAN Financial Innovation Network (AFIN), BCG FinTech Control Tower, and Affinidi to launch ChekFIN, a decentralised credentials platform to support partnerships between financial institutions and fintech firms. ChekFIN launched in December 2021 and seeks to enable financial institutions to obtain verified credentials of fintech firms (eg, business references, awards they have obtained, and investor funding records). These credentials are immutably stored on a blockchain as a golden source of information. Thus far, 10 global financial institutions have already signed up for ChekFIN.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

Generally, the provision of fintech products and services is predominantly regulated by the Monetary Authority of Singapore (MAS), Singapore's central bank and financial regulatory authority. Particular aspects relating to competition and data privacy issues may be specifically regulated by the Competition and Consumer Commission of Singapore and the Personal Data Protection Commissioner. The Intellectual Property Office of Singapore has also launched a fintech fast-track initiative to expedite the file-to-grant process for fintech patent applications.

MAS has launched various initiatives pertaining specifically to fintech, such as the FinTech and Innovation Group and FinTech Regulatory Sandbox. MAS has also promulgated regulations relating to aspects of fintech. Many payment companies, digital asset exchanges and other fintech ecosystem entities also fall within the scope of the Payment Services Act 2019 (the PS Act), which is regulated by MAS.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Depending on the nature and scope of services or products offered, licensing requirements under the Securities and Futures Act 2001 (SFA) or the Financial Advisers Act 2001 (FAA), or both, may apply.

The following activities are regulated under the SFA:

- dealing in capital markets products;
- advising on corporate finance;
- fund management;
- real estate investment trust management;
- product financing;
- providing credit rating services; and
- providing custodial services for specified products.

The following activities are regulated under the FAA:

- advising others, either directly or through publications or writings, and whether in electronic, print or other form, concerning any investment product, other than:
    - in the manner set out in (2); or
    - advising on corporate finance within the meaning of the SFA; and
- advising others by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product; and
- arranging any contract of insurance in respect of life policies, other than a contract of reinsurance.

The licensing requirements under the SFA and the FAA have extraterritorial effect. Section 339 of the SFA and section 90 of the FAA provide that where a person does an act partly in and partly outside Singapore, which, if done wholly in Singapore, would constitute an offence against any provision of the SFA or the FAA (as the case may be), that person shall be guilty of that offence as if the act were carried out by that person wholly in Singapore, and may be dealt with as if the offence was committed wholly in Singapore. In addition, section 339 of the SFA also provides that where a person does an act outside Singapore that has a substantial and reasonably foreseeable effect in Singapore and that act would, if carried out in Singapore, constitute an offence under the relevant provisions of the SFA, that person shall be guilty of that offence as if the act were carried out by that person in Singapore, and may be dealt with as if the offence were committed in Singapore.

Read this article on Lexology

The activity most relevant to fintech businesses is likely to be 'dealing in capital markets products' under the SFA. 'Dealing in capital markets products' means (whether as principal or agent) making or offering to make with any person, or inducing or attempting to induce any person to enter into or to offer to enter into any agreement for or with a view to acquiring, disposing of, entering into, effecting, arranging, subscribing for, or underwriting any capital markets products. 'Capital markets products' means any securities, units in a collective investment scheme, derivatives contracts, spot foreign exchange contracts for the purposes of leveraged foreign exchange trading, and such other products as MAS may prescribe as capital markets products.

In addition to the above licensing requirements, where a fintech business undertakes banking business, such as receiving money on current or deposit accounts, this business is required to be licensed as a bank by MAS pursuant to the Banking Act 1970 (BA). Similarly, if the fintech business undertakes the business of moneylending or promotes doing so, it will require a licence pursuant to the Moneylenders Act 2008 (MLA), unless it is an excluded moneylender or an exempt moneylender.

Since 28 January 2020, the PS Act has come into force. Under the PS Act, where a fintech business carries on a business of providing any type of payment service in Singapore, it must have a licence that entitles it to do so in respect of that type of payment service or be an exempt payment service provider with respect to that type of payment service. Each of the following services is a payment service for the purposes of the PS Act:

- account issuance service;
- domestic money transfer service;
- cross-border money transfer service;
- merchant acquisition service;
- e-money issuance service;
- digital payment token service; and
- money-changing service.

In general, licensing requirements may differ depending on the nature and scope of activities contemplated, and advice should be sought on the specific circumstances of any particular case.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Under Singapore law, the offering and provision of consumer lending is not distinguished from primary lending. Lending (consumer lending and primary lending) is a regulated activity in the jurisdiction and is governed by the MLA.

The MLA requires that all loans made available in Singapore are by licensed moneylenders or excluded moneylenders. Examples of excluded moneylenders are:

- any person regulated by MAS under any other written law who is permitted or authorised to lend money or is not prohibited from lending money under that other written law;
- any person who lends money solely to his or her employees as a benefit of employment;

- any person who lends money solely to accredited investors within the meaning of section 4A of the SFA of Singapore; and
- any person carrying on any business not having as its primary object the lending of money in the course of which and for the purposes whereof he or she lends money.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

The acquisition of a (funded) loan receivable and the holding of that loan receivable does not constitute moneylending unless, following the acquisition, additional loans are extended.

Secondary market loan intermediation is not a regulated activity, provided that it does not involve any lending or deposit taking and provided that loans are not in the form of securities.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Broadly, 'collective investment schemes' are arrangements in respect of any property that exhibit the following features:

- the participants do not have day-to-day control over the management of the property (Control Limb);
- the property is managed as a whole by or on behalf of a manager (Management Limb) or the contributions of the participants, or both, and the profits or income out of which payments are to be made to the participants are pooled (Pooling Limb); and
- the purpose or effect (or purported purpose or effect) of the arrangement is to enable participants to participate in or receive profits, income, or other payments or returns arising from the acquisition, holding, management, disposal, exercise, redemption or expiry of, any right, interest, title, or benefit in the property or any part of the property or to receive sums paid out of such profits, income, or other payments or returns (Purpose Limb).

Previously, it was a requirement that both the Management Limb and the Pooling Limb be satisfied. However, following certain amendments to the laws in October 2018, arrangements can now qualify as a 'collective investment scheme' if they fulfil either the Management Limb or the Pooling Limb, or both, in addition to the Control Limb and Purpose Limb.

Generally, unless an exemption applies, it is an offence to make an offer of units in a collective investment scheme to the Singapore public unless the scheme is authorised or recognised by MAS and the offer is made in or accompanied by an SFA-compliant prospectus.

It is possible that certain fintech activities could involve a collective investment scheme where the business concerned is managing assets on behalf of participants who have invested through a fintech platform. Careful analysis of the specific circumstances and the

way in which the platform permits investors to participate will be required to determine whether it constitutes a collective investment scheme.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

Managing the property of or operating a collective investment scheme or undertaking on behalf of a customer (whether on a discretionary authority granted by the customer or otherwise) is regulated as 'fund management' under the SFA if it involves:

- the management of a portfolio of capital markets products; or
- the entry into spot foreign exchange contracts for the purpose of managing the customer's funds, but not including real estate investment trust management.

Accordingly, unless an exemption applies, managers of alternative investment funds generally require a licence to conduct business involving these activities.

Peer-to-peer and marketplace lending

9 | Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

There are no specific regulations applicable to peer-to-peer or marketplace lending in Singapore. Fundraising from the public through lending-based crowdfunding, or peer-to-peer lending, is regulated by MAS under the SFA and the FAA. Therefore, such activity might constitute a regulated activity that requires a licence, but much will depend on the precise model.

Further, in Singapore, any invitation to lend money to an entity is deemed to be an offer of debentures, which is a type of security. The entity offering the debentures is required to prepare and register an SFA-compliant prospectus with MAS unless an exemption applies.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

There are specific regulations applicable to crowdfunding in Singapore. These regulations apply to securities-based crowdfunding operators (both equity-based crowdfunding and lending-based crowdfunding).

Generally, securities-based crowdfunding is regulated by MAS under the SFA and the FAA, and would likely constitute a regulated activity that requires a licence.

As for lending-based crowdfunding in particular, guidance has been provided under MAS's FAQ on Lending-Based Crowdfunding (issued on 8 October 2018). While the FAQs do not introduce new rules, the FAQs do clarify the applicability of the SFA or the FAA to lending-based crowdfunding.

If applicable, the SFA would require a lending-based crowdfunder to register a prospectus with MAS, unless exempted. It would only be exempted if the crowdfunding offer is:

- a personal offer (made only to pre-identified persons) of no more than S$5 million within a 12-month period;
- a private placement to no more than 50 investors within a 12-month period; or
- an offer made only to institutional investors, or accredited investors but subject to certain conditions.

These are no unique exemptions and generally exist under the SFA in respect of security offerings.

Separately, if the operator provides financial advice to interested investors, the operator would also need to comply with the requirements of the FAA.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

To the extent that an invoice is purchased, without risk of being recharacterised as a loan for the purposes of the MLA, with true sale there is no specific regulation on the buying and selling of invoices. This is common in factoring and invoice discounting arrangements.

However, if invoices are opened to the public and crowdfunded, then depending on the precise nature of the crowdfunding scheme and the manner in which it is carried out (specifically if such invoices are structured as debt securities), then the operator of the trading platform will likely need to abide by the usual provisions under the SFA and the FAA (if applicable).

Payment services

12 | Are payment services regulated in your jurisdiction?

Payment services include a wide range of activities, such as taking cash deposits, making cash withdrawals, executing payment transactions, issuing or acquiring payment instruments, issuing and administering means of payment, money remittance, making payments sent through the intermediary of a telecoms, IT system or network operator, or even providing stored value facilities.

Since 29 January 2020, seven payment services are now regulated in Singapore under the PS Act:

- account issuance service;
- domestic money transfer service;
- cross-border money transfer service;
- merchant acquisition service;
- e-money issuance service;
- digital payment token service; and
- money-changing service.

To carry on the business of providing any of the above-mentioned payment services, the entity will require one of three types of licences: a money-changing licence, standard payment institution licence or major payment institution licence.

Different regulatory conditions apply to each type of licence, with the extent of regulatory conditions increasing from standard payment institutions to major payment institutions. For instance, major payment institutions must safeguard customer money with an undertaking by a bank or prescribed financial institution, a guarantee by a bank or prescribed financial institution or segregate customer money in a trust account maintained by a bank or prescribed financial institution. On the other hand, standard payment institutions are not subjected to these safeguarding measures, although they must alert customers so they can make informed decisions.

Correspondingly, each of these licences authorises the licensee to conduct different types and transaction volumes of each type of payment service. For example, standard payment institutions may carry on business so long as the monthly transactions for any activity type do not exceed S$3 million, the monthly transactions for two or more activity types do not exceed S$6 million and, where relevant, the total amount of daily outstanding e-money does not exceed S$5 million. In contrast, the quantum limits applicable to standard payment institutions do not apply to major payment institutions.

The PS Act includes provisions to mitigate the risks of loss of customer monies, money laundering and terrorism financing risks, fragmentation and lack of interoperability across payment solutions, and technology risks including cyber risks. MAS has also proposed technology risk management requirements, including cybersecurity risk management guidelines.

Under the Payment Services (Amendment) Bill 2021 passed on 4 January 2021, amendments relating to anti-money laundering and countering terrorist financing (AML/CTF), cross-border money transfer services and digital payment token (DPT) services have been introduced. The scope of DPT services has been significantly increased to address Singapore's commitment to the Financial Action Task Force standards. MAS has stated that it intends to grant a six-month exemption to entities that are newly regulated under the PS Act, as well as to existing PS Act-licensed entities that have to change their licences as a result of the amendments.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

MAS has published a comprehensive application programming interface (API) playbook in its bid to encourage more banks to participate in open banking. This document outlines and standards framework for:

- API governance;
- API lifecycle governance;
- governance of API risk; and

- regulatory considerations for partner API operating models.

The result of MAS's push towards open banking can be clearly seen with businesses such as Citibank, DBS, OCBC, Standard Chartered and payments service provider NETS running their own Open API portals comprising over 272 API sets.

MAS has also implemented the Financial Industry API Register, which is updated semi-annually and designed to serve as the initial landing site for Open APIs in the Singaporean finance industry. These APIs fall under the following functional categories:

- product APIs that provide information on financial product details, rates and branch or automatic teller machine locations;
- sales and marketing APIs for product sign-ups, sales or cross-sales and leads generation;
- servicing APIs for managing customer profiles or account details and customer queries or feedback;
- transaction APIs that support customer instructions for payments, funds transfers, settlements, clearing, trade confirmations and trading;
- other APIs for common services, such as authentication, authorisation, reporting, market data and compliance; and
- regulatory APIs that enable extraction of data sets related to the financial industry as a whole.

On 14 May 2020, the Personal Data Protection Commission and the Ministry of Communications and Information launched a public consultation paper where it proposed to introduce a new Data Portability Obligation to give individuals greater choice and control over their personal data, prevent consumer lock-in and enable switching to new services. Data portability allows individuals to request an organisation to transmit a copy of their personal data to another organisation.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Robo-advisers and other companies that provide retail customers with automated access to investment products in Singapore are regulated under the SFA or the FAA, or both, and must adhere to MAS's Guidelines on Provision of Digital Advisory Services (CMG-G02) (the Advisory Guidelines), including the requirement to be appropriately licensed unless they qualify for relevant exemptions.

However, as MAS is keen not to stifle digital innovation, the Advisory Guidelines provide for a lower bar for licensing in certain circumstances. For example, digital advisers that seek to offer fund management services to retail investors will be eligible for licensing even if they do not meet the SFA corporate track record requirements, provided they meet other specified safeguards.

Read this article on Lexology

Under the Advisory Guidelines, digital advisers will be exempted from the FAA requirement to collect the full suite of information on the financial circumstances of a client, such as income and financial commitments. This is on the condition that they put in place measures to mitigate the risks of providing unsuitable investment recommendations owing to limited client information.

While MAS is making it easier for digital advisers to set up in Singapore, the business model carries unique risks, such as faulty algorithms and cyber threats. To mitigate these risks, the Advisory Guidelines set out MAS's expectations for digital advisers to establish robust frameworks to govern and supervise their algorithms, as well as to manage technology and cyber risks.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

The marketing and sale of insurance products are regulated under the Insurance Act 1966 and the FAA.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Credit bureaus are recognised by MAS under the BA to collect and disclose credit data to their members. On 31 May 2021, the Credit Bureau Act 2016 (CBA) came into effect, under which there is a framework in place to subject credit bureaus to formal supervision by MAS, as credit bureaus collect increasing (and more specifically detailed) amounts of data to facilitate more comprehensive credit assessments by their members. The CBA also allows consumers the right to access, review and rectify their credit records. The provision of credit ratings (opinions primarily regarding the creditworthiness of entities other than individuals, governments or securities) is also regulated under the SFA.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

No.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

There is no general approach towards fintech companies, and it depends on exactly what type of financial service is being provided by the company, and the requirements under the corresponding legislation (eg, Securities and Futures Act 2001, Payment Services Act, Banking Act 1970, etc).

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

This will depend on many factors, including but not limited to the regulatory status of the financial institution (eg, whether the financial institution is licensed or exempt and the type of licence held or exemption being relied upon) and the types of services and products being marketed. Depending on the facts, different rules and restrictions may need to be taken into account, including, for example, clientele restrictions.

Advice should be sought on the specific circumstances of any particular case.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

There are no specific regulations or guidelines in relation to the use of distributed ledger technology (DLT) in Singapore. However, the Monetary Authority of Singapore (MAS), has been encouraging the industry to look at DLT in relation to the financial system in Singapore. For example, in early 2017, MAS announced the successful conclusion of the proof-of-concept project to conduct domestic interbank payments using DLT, and in late 2017, an industry consortium led by MAS and the Association of Banks in Singapore released source codes of successful DLT prototypes publicly to encourage innovation in interbank payments.

The most relevant legislation in respect of DLT and (or) blockchain technology would be the PS Act, under which digital payment token (DPT) service providers (such as traders and exchanges) would require a licence.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

Generally, whether a particular cryptoasset is regulated, and how it would be regulated, would depend on the nature and characteristics of such cryptoasset. For example, if a cryptoasset is a security, it would likely fall within the scope of the Securities and Futures Act 2001 (SFA); if a cryptoasset is a DPT (such as stablecoins), it would likely fall within the scope of the PS Act.

In many cases, the PS Act applies, which currently regulates the dealing in (buying and selling) DPTs, and facilitating the exchange of DPTs. However, under the Payment Services (Amendment) Bill 2021, which was passed on 4 January 2021 but has yet to come into force, the scope of DPT services will be expanded to capture a few more types of regulated activities in relation to DPTs. In this regard, MAS has stated that any entities that are already carrying on such business activities will be given six months, after the Payment Services (Amendment) Act 2021 comes into force, to make the necessary licence applications.

In January 2022, MAS issued guidelines to discourage cryptocurrency trading by the general public. The new guidelines clarify MAS' expectations that DPT service providers should not engage in marketing or advertising of DPT services:

- in public areas in Singapore such as through advertisements on public transport, public transport venues, public websites, social media platforms, broadcast and print media, or provision of physical automated teller machines; or
- through the engagement of third parties, such as social media influencers, to promote DPT services to the general public in Singapore.

DPT service providers are limited to marketing and advertising their services on their own corporate websites, mobile applications or social media accounts. These guidelines emphasise MAS' stance that 'the trading of cryptocurrencies is highly risky and not suitable for the general public'.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

There are no specific rules or regulations governing the issuance of digital tokens per se. Whether a particular cryptoasset is regulated, and how it would be regulated, would depend on the nature and characteristics of such cryptoasset. In the case of security token offerings, the SFA would apply where such digital tokens are security tokens, which would likely give rise to a licensing obligation and (or) the need to register a prospectus.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

Strictly speaking, there are no hard rules or regulations specific to artificial intelligence (AI). However, the Monetary Authority of Singapore (MAS), has issued various publications aimed at fostering the development of AI innovation, as well as addressing potential issues.

For example, MAS has published a set of principles to promote fairness, ethics, accountability and transparency (FEAT) in the use of AI and data analytics in finance. Known as the FEAT Principles, the document provides guidance to firms offering financial products and services on the responsible use of AI and data analytics, to strengthen internal governance around data management and use.

MAS has said that this is intended to foster greater confidence and trust in the use of AI and data analytics, as firms increasingly adopt technology tools and solutions to support business strategies and in risk management.

With regard to robo-advice, robo-advisers are not regulated separately. Depending on the scope of the service being provided (eg, whether the digital adviser exercises active discretion, as opposed to mere automated portfolio rebalancing, and (or) whether the digital adviser actually provides advice and (or) recommendations on investment decisions), a robo-adviser may need to be licensed under one or more of the existing licensing regimes (eg, as a fund manager, as a financial adviser, etc)

While MAS is making it easier for digital advisers to set up in Singapore, the business model carries unique risks, such as faulty algorithms and cyber threats. To mitigate these risks, the Guidelines on Provision of Digital Advisory Services (the Advisory Guidelines) set out MAS's expectations for digital advisers to establish robust frameworks to govern and supervise their algorithms, as well as to manage technology and cyber risks.

In May 2020, MAS announced the first phase of its Veritas initiative, which is a framework for the responsible adoption of AI and data analytics by financial institutions. Phase 1 of Veritas was concluded in January 2021, which concerned the development of the fairness metrics, and Phase 2 was concluded in February 2022 with the issuance of five whitepapers that included a FEAT checklist for financial institutes to adopt for software development, and the assessment methodologies regarding enhanced fairness, ethics and accountability and transparency.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Different consent requirements apply to the acquisition of different types of regulated businesses. In general, where a person is to become a holder of a specified percentage of a regulated entity or will control a specified percentage of voting rights of that entity, prior consent must be obtained from the relevant regulatory authority.

In all cases, advice should be sought as to the applicable requirements and the process for obtaining consent.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Under the PS Act, digital payment token service providers will have to be licensed, and will have to abide by their anti-money laundering and countering the financing of terrorism (AML/CFT) obligations under the PSA.

Such AML/CFT requirements oblige licensees to take appropriate steps to identify, assess and understand their money laundering and terrorism financing (ML/TF) risks, and develop and implement policies, procedures and controls for the effective management of these risks.

This includes policies, procedures and controls in relation to customer due diligence, transaction monitoring, screening, suspicious transactions reporting and record-keeping. Enhanced measures should be performed where higher ML/TF risks are identified.

The requirements also include monitoring the implementation of policies, procedures and controls, and enhancing them if necessary.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no specific guidance for fintech companies, but there is guidance for regulated companies and banks that would apply to fintech businesses that are regulated similarly.

Specifically for digital asset exchanges, the Association of Cryptocurrency Enterprises and Start-ups Singapore has developed a Code of Practice under its Standardisation of Practice In Crypto Entities initiative.

Read this article on Lexology

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

There are no legal requirements or regulatory guidance relating to personal data that are specifically aimed at fintech businesses. However, fintech companies must have regard to Chapter 6 on Online Activities of the Personal Data Protection Commissioner's (PDPC) Advisory Guidelines on the Personal Data Protection Act (PDPA) for Selected Topics.

The PDPC has announced different initiatives to facilitate the movement and use of data to support innovation and strengthen accountability among organisations. The first is the PDPC's response note to the public consultation on proposed data portability and data innovation provisions, as part of the review of the PDPA. The data portability provision provides individuals with greater control over their personal data and enables greater access to more data by organisations to facilitate data flows and increase innovation, while the data innovation provision makes it clear that organisations can use data for appropriate business purposes without individuals' consent.

The second is the PDPC's introduction of a series of guides, such as:

- the Guide on Active Enforcement, as part of its drive for organisations to shift from compliance to accountability;
- an updated Guide to Managing and Notifying Data Breaches under the PDPA, to help organisations manage and respond to data breaches more effectively; and
- the Guide to Notification, which illustrates good notification practices for organisations to comply with their Notification Obligations under the PDPA.

On 1 February 2021, certain key amendments to the PDPA, as well as accompanying subsidiary regulations, came into force. This round of amendments will introduce significant change to the existing data protection regime in Singapore, which bring it closer in line with higher global standards.

Examples of amendments include:

- an increase in financial penalty for breaches of the PDPA to S$1 million;
- the introduction of a mandatory data breach notification requirement;
- new exceptions to consent – legitimate interests and business improvement;
- expanded scope of deemed consent; and
- new personal liability for mishandling of personal data.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

While there is a cybersecurity law, the Cybersecurity Act 2018, that came into force in August 2018, it is unlikely to directly affect unregulated fintech start-ups as it is intended

to regulate systems involved in the provision of essential services within Singapore. The Cybersecurity Act provides an overarching legislative framework for the regulation of owners of critical information infrastructure and cybersecurity service providers.

In September 2018, the Monetary Authority of Singapore (MAS), sought to strengthen the rules on cyber security through its Notice on Cyber Hygiene in view of the deepening cyber threat landscape and to further strengthen the overall cyber resilience of financial institutions. It intends to eventually prescribe a set of legally binding essential cyber security practices that financial institutions must put in place to manage cyber threats, which could include:

- addressing system security flaws in a timely manner;
- establishing and implementing robust security for systems; and
- deploying security devices to secure system connections.

With regard to regulated fintech companies, MAS also expanded the Technology Risk Management Guidelines following a consultation in March 2019, and added the following guidance:

- technology risk governance and oversight;
- best practices for software development;
- additional guidance for new technologies (namely, application programming interfaces, smart electronic devices and virtualisation); and
- effective cyber surveillance, secure software development, adversarial attack simulation and management of cyber risks posed by the internet of things.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

On 5 October 2018, the Monetary Authority of Singapore (MAS), issued revised Guidelines on Outsourcing. Various industry guidelines on outsourcing have also been issued by the Investment Management Association of Singapore and the Association of Banks in Singapore.

MAS Guidelines on Outsourcing set out risk management practices to be complied with when a regulated entity has entered into any outsourcing or is planning to outsource its business services to a service provider (whether this outsourcing is done on an intra-group or a third-party basis, or a material or non-material basis). Certain key requirements in the Outsourcing Guidelines include maintaining an Outsourcing Register and ensuring that all outsourcing contracts are written agreements containing the minimum prescribed clauses. The Outsourcing Guidelines also detail the responsibilities of the board and senior management in this regard (eg, approving a risk evaluation framework, setting a suitable risk appetite statement, laying down appropriate approval authorities, assessing management

competencies to develop sound and responsive outsourcing risk management policies and procedures that are commensurate with the nature, scope and complexity of the outsourcing arrangements).

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

Yes, financial institutions regulated by MAS should have regard mainly to MAS Guidelines on Outsourcing. MAS considers cloud services operated by service providers to be a form of outsourcing. In this respect, MAS also considers that the types of risks in cloud services that confront institutions are not necessarily distinct from that of other forms of outsourcing arrangements. Accordingly, institutions should still perform the necessary due diligence and apply sound governance and risk management practices required by the Outsourcing Guidelines when subscribing to cloud services.

Nevertheless, to the extent that cloud services have certain typical characteristics, such as multi-tenancy, data commingling and the higher propensity for processing to be carried out in multiple locations, institutions should take measures to address those risks, bearing in mind the materiality of those risks specific to each institution. In this regard, the institution would have to deal with risks associated with data, to ensure the service provider can identify and segregate customer data, and robust access controls to protect customer information.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Computer programs (and preparatory design materials for computer programs) are protected by copyright as literary works under the Copyright Act (Chapter 63). Copyright arises automatically as soon as the computer program is recorded. Registration of copyright is not required and is not possible in Singapore.

If the software code has been kept confidential it may also be protected as confidential information. No registration is required.

Patents for software (source code) are not currently applicable for patent registration and protection. The Intellectual Property Office of Singapore (IPOS) has issued the Examination Guidelines for Patent Applications at IPOS, which takes the view that 'claims to software that are characterised only by source code, and not by any technical features, is unlikely to be considered an invention on the basis that the actual contribution would be a mere presentation of information'.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Copyright created by an employee in the course of his or her employment is automatically owned by the employer unless otherwise agreed.

An invention made by an employee belongs to the employer if it was made in the course of the normal duties of the employee or in the course of duties falling outside his or her normal duties, but specifically assigned to him or her, and the circumstances, in either case, were such that an invention might reasonably be expected to result from the carrying out of his or her duties; or if the invention was made in the course of the duties of the employee and, at the time of making the invention, because of the nature of his or her duties and the particular responsibilities arising from the nature of his or her duties, he or she had a special obligation to further the interests of the employer's undertaking.

Except in certain narrow circumstances, copyright or inventions created by contractors or consultants in the course of their duties are owned by the contractor or consultant unless otherwise agreed in writing.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Yes, unless amended by agreement, joint owners of a copyright hold their shares as tenants in common. Any use, licence, charge or assignment of the copyright must, therefore, be done by the joint owners as a whole or by one of the joint owners with the consent of the other joint owners.

However, this position is different for patents notwithstanding that these co-owners hold the ownership of the patent as tenants-in-common. Except where the statutory provisions have been amended by agreement between the joint owners, the Patents Act provides that a co-owner is entitled to do any otherwise infringing act for his or her own benefit, by him or herself or by his or her agents, without requiring the consent of (or the need to account to) any of the other co-owners.

Nevertheless, a co-owner may not, without the consent of the other co-owners, grant a licence under the patent or assign or charge a share in the patent.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Confidential information can be protected against misuse, provided the information in question has the necessary quality of confidence, is subject to an express or implied duty of

confidence, or no registration is necessary (or possible). Confidential information can be kept confidential during civil proceedings with the permission of the court.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brands can be protected as registered trademarks in Singapore. A brand can also be protected under the common law tort of passing off if it has acquired sufficient goodwill.

Certain branding, such as logos and stylised marks, can also be protected by design rights and may also be protected by copyright as artistic works.

The IPOS trademark database can be searched to identify potentially problematic trademarks that have been registered or applied for.

It is highly advisable for new businesses to conduct trademark searches to check whether earlier registrations exist that are identical or similar to their proposed brand names. It may also be advisable to conduct internet searches for any unregistered trademark rights that may prevent the use of the proposed mark.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

Remedies include:

- preliminary and final injunctions;
- damages or an account of profits;
- delivery up or destruction of infringing products;
- disclosure orders; and
- costs.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

There is a competition regime in Singapore that applies to all entities carrying out business in Singapore unless otherwise exempted. There are no particular aspects of this regime that would affect fintech businesses disproportionately to other businesses.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

At present, there are no tax incentives specifically targeted at fintech companies. However, new start-up companies in general can benefit from a tax exemption scheme. All companies are eligible for the exemption except companies whose principal activity is investment holding and companies that undertake property development for sale, investment or both. To qualify for the exemption, an eligible company must:

- be incorporated in Singapore;
- be tax-resident in Singapore for the relevant tax year of assessment; and
- have its share capital held by no more than 20 persons (all of whom must be individuals) throughout the period of that tax year of assessment, where at least one shareholder is an individual holding at least 10 per cent of the shares in the company, typically a founder.

The exemption applies for the company's first three consecutive tax years of assessment. With effect from tax year of assessment 2020, companies will benefit from a reduced 75 per cent exemption from tax on the first S$100,000 of normal chargeable income and then a 50 per cent exemption on the next S$100,000 of normal chargeable income.

Under the Angel Investors Tax Deduction Scheme, investors who are able to commit a minimum of S$100,000 of investment to a qualifying start-up can, subject to approval and satisfaction of certain conditions, benefit from a tax deduction of 50 per cent of the amount of their investment at the end of a two-year holding period. This scheme lapsed after 31 March 2020, and investors can no longer obtain new approvals or renewal of the 'angel investor' status for any period commencing after 31 March 2020. However, angel investors will continue to enjoy tax deductions in respect of qualifying investments made during the period of the approved status, subject to existing conditions of the scheme.

For institutional investors, section 13H of the Income Tax Act allows approved venture capital and private equity funds to benefit from zero-rated tax relief for up to 10 years in respect of gains from the divestment of approved portfolio holdings, dividend income from approved foreign portfolio holdings and interest income arising from approved foreign convertible loan stock. In addition, the Fund Management Incentive (FMI) gives an approved fund management company tax relief at a concessionary rate of 5 per cent for a period of up to 10 years in respect of both management fees and performance bonuses received from an approved venture capital fund. To benefit from both section 13H and the FMI, the venture capital or private equity funds and fund management companies must, at a minimum, be incorporated and based in Singapore and otherwise approved or licensed by the Monetary Authority of Singapore to conduct their activities.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

Yes, the Goods and Services Tax Act was amended in 2020 to require overseas digital service providers with a yearly global turnover of more than S$1 million, which sell more than S$100,000 worth of digital services to customers in Singapore in a 12-month period, to register for and charge goods and services tax (GST).

With effect from 1 January 2020, the Inland Revenue Authority of Singapore has required these digital services providers, who are registered under this Overseas Vendor Registration regime, to charge GST on their sale of digital services to Singapore consumers.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

The rules on hiring staff from abroad apply to all companies operating in Singapore. Prior to applying for an Employment Pass, companies will need to advertise the vacancy on the National Jobs Bank for at least 14 days unless a specific exemption applies.

The Economic Development Board launched Tech.Pass, a targeted programme to attract tech entrepreneurs, leaders and technical experts from around the world with experience in established or fast-growing tech companies, to contribute to the development of Singapore's tech ecosystem. Tech.Pass will allow passholders flexibility in the participation of activities such as starting and operating one or more tech companies, being an investor, employee or director in one or more Singapore-based companies or a consultant (or) mentor mentoring start-ups and lecturing at local universities.

UPDATE AND TRENDS

Current developments

41 Are there any other current developments or emerging trends to note?

On 28 June 2019, the Monetary Authority of Singapore (MAS) announced that it will issue up to five new digital banking licences, welcoming applications from both traditional banking groups and non-bank players. The move has been recognised as marking the next chapter in Singapore's banking liberalisation journey.

In early December 2020, MAS announced that four entities were awarded digital banking licences.

Read this article on Lexology

While digital banks offer the same banking services as traditional banks, they operate without a physical setup, enabling customers to control their finances from their computers or smartphones. MAS awarded the licences to:

- a consortium of Singapore Telecommunications Ltd (Singtel) and Grab Holding Inc (Grab);
- Sea Limited;
- Ant Financial; and
- a consortium of Greenland Financial Holdings Group Co Ltd, Linklogis Hong Kong Ltd, and Beijing Co-operative Equity Investment Fund Management Co Ltd.

There are two types of digital banking licences – digital full bank licence (DFB) and digital wholesale bank licence (DWB).

The DFB licence enables an entity to offer deposits, loans and investment products through its online platform. DFB licence holders can only serve retail and corporate banking services while DWB licence holders can only serve businesses, namely small and medium enterprises (SMEs).

MAS expects the four digital banks to commence operations by early 2022. This is the first time Singapore has approved setting up wholly digital banking operations.

On 5 April 2022, Parliament passed the Financial Services and Markets Act 2022 (the FSM Act), although it has yet to come into force. The FSM Act enhances MAS's regulatory and enforcement framework across the entirety of the financial sector, adding to the rules designed for each specific segment. The FSM Act also ensures that digital token service providers that are Singapore entities, but who wholly operate outside of Singapore, would be captured within the scope of Singapore's regulatory regime, bringing Singapore's legal and regulatory framework in respect of virtual asset service providers in line with the Financial Action Task Force standards.

In October 2022, MAS published two consultation papers proposing regulatory measures (which would, if adopted, form part of the PS Act) for DPT services and stablecoins, to reduce the risk of consumer harm from the trading of cryptoassets and to support the development of stablecoins as a credible medium of exchange.

The proposed measures regarding digital payment token (DPT) services would require DPT service providers:

- to provide adequate risk disclosures to help retail consumers to make informed cryptocurrency trading decisions; and
- to implement proper systems to safeguard customers' assets, mitigate potential conflicts of interest and account for technology risks.

In relation to stablecoins, MAS proposes to regulate the issuance of single-currency pegged stablecoins (SCS) while stablecoins pegged to a basket of currencies or other assets (eg, commodities) will be subject to the existing DPT regime under the PS Act. Under the proposed regulatory regime, SCS issuers will be subject to higher prudential standards and will be required to make disclosures (or even a key information factsheet as a matter of good

Read this article on Lexology

practice) on its corporate website, disclosing descriptions of the SCS, rights and obligations of the SCS issuer and holder, as well as risk factors.

MAS is currently processing the feedback from the two consultations and is likely to be issuing new guidelines for the proposed regulatory measures.

Ying Wang yingyu.wang@simmons-simmons.com
Ashleigh Low ashleigh.low@simmons-simmons.com

168 Robinson Road, 11-01 Capital Tower, Singapore 068912, Singapore
Tel: +65 6831 5600
www.simmons-simmons.com

Read more from this firm on Lexology

Read this article on Lexology

South Korea

Juho Yoon, Young Ju Park, Se Yeong Im and Jinhee Rhew

Bae, Kim & Lee LLC

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 484

General innovation climate 484
Government and regulatory support 485

FINANCIAL REGULATION 485

Regulatory bodies 485
Regulated activities 486
Consumer lending 486
Secondary market loan trading 487
Collective investment schemes 487
Alternative investment funds 487
Peer-to-peer and marketplace lending 487
Crowdfunding 488
Invoice trading 488
Payment services 488
Open banking 488
Robo-advice 489
Insurance products 489
Credit references 489

CROSS-BORDER REGULATION 489

Passporting 489
Requirement for a local presence 490

SALES AND MARKETING 490

Restrictions 490

CRYPTOASSETS AND TOKENS 491

Distributed ledger technology 491
Cryptoassets 491
Token issuance 492

ARTIFICIAL INTELLIGENCE 492

Artificial intelligence 492

CHANGE OF CONTROL 493

Notification and consent 493

Read this article on Lexology

FINANCIAL CRIME	**493**
Anti-bribery and anti-money laundering procedures	493
Guidance	494
DATA PROTECTION AND CYBERSECURITY	**494**
Data protection	494
Cybersecurity	495
OUTSOURCING AND CLOUD COMPUTING	**496**
Outsourcing	496
Cloud computing	497
INTELLECTUAL PROPERTY RIGHTS	**498**
IP protection for software	498
IP developed by employees and contractors	498
Joint ownership	499
Trade secrets	499
Branding	499
Remedies for infringement of IP	500
COMPETITION	**500**
Sector-specific issues	500
TAX	**500**
Incentives	500
Increased tax burden	501
IMMIGRATION	**501**
Sector-specific schemes	501
UPDATE AND TRENDS	**502**
Current developments	502

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

In South Korea, various fintech companies are actively engaged in promoting and operating their business, and many traditional financial companies are striving to expand their business presence within the fintech industry.

To create momentum for fintech innovation, the South Korean government operates a regulatory sandbox programme pursuant to the Special Act on Support for Financial Innovation, which took effect on 1 April 2019. As of May 2023, a total of 292 projects have been designated to benefit from regulatory exemptions.

Recently, the virtual asset industry has been undergoing meaningful changes at a rapid pace. For example, a bill on the Act on the Protection of Virtual Asset Investors is expected to be passed in the National Assembly soon. The bill focuses on enhancing the protection

Read this article on Lexology

of virtual asset investors by introducing certain obligations of virtual asset service providers and prohibiting unfair practices related to cryptoasset transactions.

In addition, in February 2023, the Financial Services Commission (FSC) introduced policies and guidelines on the issuance and circulation of security tokens to permit security token offerings. According to the policies and guidelines:

- distributed ledger technology will be legally recognised as a method of registering official records of information regarding the occurrence, change and expiration or termination of rights pertaining to a security; and
- a new licence for over-the-counter trading platforms for securities tokens (more specifically, investment contract securities and certificates on non-money trusts) will be introduced in due course.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

To support financial innovation, the regulatory sandbox programme was introduced in 2019, which exempts, either fully or partially, eligible fintech companies from various restrictions under financial-related laws (including permits and approval requirements). This exemption will be granted for up to two years as a general rule and may be extended once for another two years.

Additionally, in 2018, the Special Act on the Establishment and Operation of Internet-only Banks was passed to make it possible to run an online banking business without any offline (physical) branch. The same Act also relaxed regulations on IT companies' acquisition of equity shares in internet-only banks. As of the date of this submission, three internet-only banks are operating in South Korea.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

The FSC and the Financial Supervisory Service (FSS) are the two primary institutions in charge of regulatory enforcement over fintech products and services.

The FSC is a government institution mainly responsible for creating financial policies. The FSS is responsible for supervising and inspecting financial companies as the enforcement arm of the FSC.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Generally, an entity that intends to engage in any of the following businesses involving financial investment instruments must obtain licences and approvals required under the South Korean Financial Investment Services and Capital Markets Act (FSCMA). Under the FSCMA, a financial investment product is defined as a product acquired by an agreement to pay money or other assets at a specific point in the present or in the future, with the intent to earn a profit or avoid a loss, where there is a risk (namely, investment risk) that the total amount of such money or assets paid or payable, to acquire that product may exceed the total amount of money or other assets already recovered or recoverable from such product:

Classification of business	Description
Investment dealing business	Selling and purchasing financial investment instruments on its proprietary account
Investment brokerage business	Selling and purchasing financial investment instruments, broking thereof, on the account of others
Collective investment business	Pooling investment from two or more investors and managing the investment on behalf of the investors
Investment advisory business	Providing advice on the values of investable assets or on investment decisions
Discrete investment management business	Making partially or wholly discretionary investment decisions and managing the investments on behalf of customers
Trust business	Providing trust service

The deposit-taking business may only be conducted by banks (including internet-only banks) or saving banks under banking or savings banking licences under South Korean laws.

Similarly, the lending business may only be carried out by registered money lenders under the Act on Registration of Money Lending Business and Protection of Finance Users (the Lending Business Act) or financial companies authorised to provide loans under the relevant regulations.

Most payment services are governed by the Electronic Financial Transactions Act (EFTA), and different licences or registrations under EFTA may be required on a case-by-case basis, depending on their specific scope of business activity. For example, registration pursuant to EFTA may be required to issue electronic payment means, and transmission or receipt of payment information or mediation of settlement of proceeds requires a payment gateway licence.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Under the Lending Business Act, registration as a moneylender is required to conduct lending business. For loan brokers, additional registration in accordance with the Financial Consumer Protection Act (FCPA) is also required. However, credit finance companies such as banks under the Banking Act and credit specialised companies under the Credit Specialized

Financial Business Act are authorised to conduct lending business without separate money lender registration.

The Lending Business Act also regulates the maximum interest rate. The maximum interest rate for consumer lending is limited to 20 per cent per annum as of the date of this submission.

When soliciting consumers or advertising, credit finance companies and moneylenders shall comply with the standards set forth in the FCPA, which was enacted on 25 March 2021 to provide consumer protection standards for all financial products, including loans.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

Loan claims may only be acquired by entities specifically listed under the Lending Business Act, such as registered loan collection business entities, banks and credit-specialised companies.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

The collective investment business and collective investment schemes are regulated under the FSCMA. Assuming that alternative finance products or services are categorised as collective investment schemes under the FSCMA, a fintech company should obtain the relevant licence and comply with the regulations under the FSCMA.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

The collective investment schemes and their managers are regulated under the FSCMA. Assuming that alternative investment funds are categorised as collective investment funds, to manage the alternative investment funds in South Korea, the fintech company should obtain the required licence and comply with the regulations under the FSCMA.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Peer-to-peer (P2P) lending platforms should complete registration and comply with various regulations under the Online Investment-Linked Finance Act, including disclosure of financial status and business structure and prohibition from engaging in high-risk practices.

In addition, P2P lending investors are subject to investment caps that are determined in proportion to their incomes.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

Equity-based crowdfunding is governed by the FSCMA. Fintech companies that wish to provide equity-based crowdfunding services need to register with the FSC. While subject to more lenient regulations than traditional financial services, relevant regulations for promoting the crowdfunding business is also subject to several restrictions. For example, the maximum amount of investment that each company may raise through crowdfunding is 1.5 billion won per year.

Reward-based crowdfunding and donation-based crowdfunding are not subject to special restrictions. However, depending on the specifics of their business model, reward-based crowdfunding business entities may be required to register as mail-order distributors under the Act on the Consumer Protection in Electronic Commerce.

Invoice trading

11 Describe any specific regulation of invoice trading in your jurisdiction.

Invoice trading is not subject to any specific regulation in South Korea.

Payment services

12 Are payment services regulated in your jurisdiction?

Payment services are mainly governed by EFTA, and any entity wishing to engage in such business should register with the FSC and comply with relevant obligations unless exempted under EFTA.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

Currently, open banking is not subject to any specific regulation in South Korea. As a general practice, financial institutions and electronic financial business entities rely on private arrangements for open banking services in cooperation with financial regulators.

For reference, there is an amendment bill for EFTA currently pending, which includes the legal grounds and requirements for open banking.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Under the FSCMA, robo-adviser services are treated as the provision of 'investment advice' subject to registration as an investment advisory service provider in principle.

In an exceptional case where another investment advisory service provider registered under the FSCMA commits to bear direct responsibilities against investors, a robo-adviser company is allowed to provide advisory services under entrustment by such investment advisory service provider without separate registration.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Any person who wishes to sell insurance products is required to be registered as an insurance agent, insurance solicitor or insurance broker under the Insurance Business Act. Further, the sale of insurance products is governed by the FCPA.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Under the Credit Information Use and Protection Act, any entity that wishes to provide credit reference or information to a third party shall obtain an appropriate licence depending on the specifics of the entity's business.

To obtain such licence, applicants must satisfy complicated requirements. For example, in most cases, licences are granted only to those entities whose 50 per cent or greater ownership is held by financial institutions (eg, banks or financial holding companies).

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

The Financial Investment Services and Capital Markets Act. was amended in 2020 to implement the Asia Region Funds Passport (ARFP). Under the ARFP, foreign passport funds registered at another ARFP member state will be available for sale in South Korea through a simplified process.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

Generally speaking, it is difficult for offshore entities to obtain a licence for financial services. However, there are exceptional cases where a local presence is not required.

For example, conducting a virtual asset-related business within South Korea requires a virtual asset service provider (VASP) registration, and this VASP registration may be filed without a local entity.

Foreign investment advisory business entities or foreign discretionary investment management business entities that provide relevant services via telecommunication may also obtain an appropriate licence without a local presence.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Financial products and services are generally regulated by the Financial Consumer Protection Act (FCPA).

In the past, sales and marketing activities used to be regulated by different laws (eg, the Banking Act and the FCPA) according to the type of business for which the sales and marketing activities are conducted. However, taking effect on 25 March 2021, the FCPA provides a uniform regulatory framework for all financial products and services.

More specifically, the FCPA applies the 'six major sales principles' to all financial products, as listed below:

Sales principle	Details
Principle of suitability	Identify a customer's information, and refrain from recommending inappropriate products
Principle of adequacy	Identify a customer's information, and if a financial product is deemed inappropriate to the customer, inform the customer of such fact and then receive the customer's confirmation of the inappropriateness
Duty to explain	Explain important matters concerning financial products to ordinary (non-professional) customers in an easily understandable manner
Prohibition of unfair practices	Refrain from performing any act infringing on a customer's rights and interests by, eg, coercing the customer to enter into an agreement for a financial product against the intent of such customer by abusing a superior position
Prohibition of misleading recommendations	Refrain from performing certain acts, such as providing assertive judgment on uncertain matters or falsely informing customers of the content of a financial product

Read this article on Lexology

Sales principle	Details
Prohibition of false or exaggerated advertisements	Refrain from making false or exaggerated advertisements

In addition, the FCPA allows ordinary customers to revoke their subscription for a financial product (with the exception of savings) within a designated time period specified for each product type, without restrictions.

If a seller of a financial product has violated any of the said principles except for the prohibition on false or exaggerated advertisements, financial customers may unilaterally terminate the sales agreement for the financial product.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

There are no laws or regulations specifically governing the use of blockchain for financial transactions.

However, certain restrictions may apply depending on the field of application of the distributed ledger technology or blockchains.

For example, the matters relating to the operation of computing systems by financial companies are prescribed in the Electronic Financial Transactions Act (EFTA) in great detail. Therefore, any system configuration, including the use of distributed ledger technology or blockchains is likely to be permitted only if it complies with EFTA.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

The regulations governing virtual assets or virtual asset service providers are prescribed in the Financial Transaction Reports Act (FTRA). Under the FTRA, virtual asset service providers, such as virtual asset exchanges and digital wallet service providers, shall register with the South Korea Financial Intelligence Unit.

The 'virtual asset' under the FTRA means 'electronically tradable or transferrable electronic tokens having an economic value', and may capture stable coins, utility tokens, and NFTs if they are deemed to have a nature of securities or payment means. For NFTs, the regulators aim to promote their growth as digital assets, mainly within the framework of the regulation for virtual assets.

In addition, a bill on the Act on the Protection of Virtual Asset Investors is expected to be passed in the National Assembly soon. The bill focuses on the protection of virtual asset investors by:

- introducing certain obligations of virtual asset service providers; and
- prohibiting unfair practices related to cryptoasset transactions.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

There are no laws or regulations specifically governing the issuance of tokens in South Korea.

The South Korean government's past position prohibited ICOs and there have been no ICOs taking place in South Korea.

In May 2022, the new administration announced its plan to permit ICOs in South Korea, with the details of the roadmap under development. Under the framework currently contemplated, the permission is likely to be granted in a limited scope for IEOs first and then gradually expanded to other types of ICOs.

In addition, in February 2023, the FSC introduced policies and guidelines on the issuance and circulation of security tokens to permit security token offerings. According to the policies and guidelines:

- distributed ledger technology will be legally recognised as a method of registering official records of information regarding the occurrence, change and expiration or termination of rights pertaining to a security; and
- a new licence for an OTC trading platform for securities tokens (more specifically, investment contract securities and certificates on non-money trusts) will be introduced in due course.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

There are no laws or regulations specifically addressing the use of artificial intelligence (AI). However, the FSC released guidelines for the use and role of AI in the financial sector in July 2021 to vitalise the use of AI in the sector and enhance the credibility in respect of AI-based financial services.

According to the guidelines, any financial companies intending to apply AI to financial transactions and customer services are required to establish an AI code of ethics, organise a body

capable of assessing and managing the potential risks of AI, and implement risk management policies.

In August 2022, the FSC announced an initiative to promote the use of AI and ensure its credibility. According to the initiative, the FSC will:

- take measures to build an AI data library for the training of AI used in the financial sector;
- build an AI testbed to support data and computing resources for the testing of AI; and
- establish an AI-based credit evaluation model and a process for verifying the security of AI-based services.

In April 2023, as a follow-up measure for the plan announced in August 2022, the FSC introduced a verification system for an AI-driven credit scoring model and an AI security guideline.

In addition, an entity that provides robo-advice services shall comply with relevant regulations under the Financial Investment Services and Capital Markets Act.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Generally, any person or entity intending to become the major shareholder of a financial company is required to obtain the Financial Services Commission's prior approval in accordance with the Act on Corporate Governance of Financial Companies or other applicable laws.

However, certain entities, such as investment advisers and discretionary investment management service providers, do not require such prior approval for the change in control concerning their shareholders. For such companies, the change in their major shareholder can be made after the change takes place.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Anti-money laundering-related matters are mainly governed by the Financial Transaction Reports Act. It applies to not only traditional financial companies but also to electronic financial business operators and virtual assets service providers.

Anti-bribery matters are regulated under various statutes, including the Criminal Act (the main criminal code of South Korea) and the Anti-Graft Act. As such, all the companies (including fintech start-ups) operating their business in South Korea must comply with such laws.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no such anti-financial crime guidance for fintech companies in South Korea.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The Credit Information Use and Protection Act (the Credit Information Act) and its subordinate regulations apply to the processing and transfer of personal credit data by fintech companies. Concurrently, the Personal Information Protection Act (PIPA) and its subordinate regulations apply.

As a general rule, fintech companies can process and (or) transfer personal (credit) data to the minimum and necessary extent upon receiving consent from a user, unless otherwise specified in other laws and regulations such as PIPA, and in the course of such processing and transfer, fintech companies need to take technical and managerial protective measures and disclose matters relevant matters in their privacy policies.

However:

- 'pseudonymised data', which makes it impossible to directly identify a data subject without using additional information can be processed without consent from the data subject, if the personal information of that data subject is collected for the purposes of preparing statistics, research or recordkeeping for public interest; and
- 'anonymised data', in which personally identifiable information is removed from data sets, is not subject to the application of regulations pursuant to the Credit Information Act and PIPA.

With respect to the foregoing, in January 2022, the Financial Services Commission (FSC) released the guidelines to be used as a reference by fintech companies in pseudonymising and anonymising personal credit data.

In addition, the amended PIPA, to take effect on 15 September 2023, will substantially modify the current framework under PIPA on transfers of personal data overseas, adding several bases for transfers that would not require data subjects' consent. Where the current PIPA allows data controllers to transfer personal data overseas with the opt-in consent of

data subjects based on detailed disclosures, the amended PIPA permits overseas transfers, without the need of obtaining the data subjects' consent, in any of the following situations:

- the transfer is by way of entrustment and details (such as the description of data transferred, country, date and method of transfer, transferee name, purpose of transfer, retention period and methods, procedures and effects of refusal to transfer) are disclosed in the privacy policy;
- the transferee has obtained an ISMS or other suitable type of certification as designated by the PIPC;
- the transfer is to a country deemed by the PIPC to satisfy PIPA levels of data protection, including as to data subjects' rights and remedy; or
- there is a treaty or agreement between the governments of South Korea and the destination country that specifically addresses personal data transfers between them.

However, note that despite the amended PIPA, financial companies are still subject to localisation regulations (prohibiting the cross-border transfer of certain information, including uniquely identifiable information).

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

The IT Network Act requires online service providers to implement a set of technical and administrative measures to ensure information security. These measures include specific requirements on formulating and operating an information security body within the company, internally establishing and complying with information security and incident response plans, making necessary investments in information security, monitoring networks and servers, and controlling online and on-site facilities access. Because fintech businesses are online service providers, they should also implement such technical and administrative measures to ensure information security.

In addition, fintech businesses are required to implement specific security arrangements and (or) technological measures under PIPA and the Credit Information Act.

Under PIPA, fintech businesses as data controllers are required to implement security arrangements including:

- to formulate and implement an internal management plan for the safe processing of personal data;
- to control access to personal information and restrict the authority to access personal data (including password protection);
- to adopt encryption technology to safely store and transmit personal data and other equivalent measures;
- to retain login records to respond to incidents of infringement with respect to personal data and to take measures to prevent the forgery and falsification thereof;
- to install and upgrade security computer programs to protect personal data; and
- to take physical measures, such as a storage or locking system, to keep personal data safe.

The Credit Information Act requires similar or potentially even higher levels of security arrangements including encryption and password protection.

Further, fintech businesses that provide specific types of services (eg, electronic fund transfer services, issuance and management of electronic debit payment and electronic prepayment and electronic payment settlement agency services) are subject to the application of the Electronic Financial Transactions Act and related requirements prescribed by the FSC with respect to:

- workforce, organisation and budget;
- facilities such as buildings, equipment, computer room, etc;
- information and technology such as terminals, electronic data, information processing systems and information and communications networks, etc; and
- other matters necessary to secure the safety of electronic financial services to ensure safety and reliability for electronic financial transactions.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Under the Regulations on Outsourcing of Business of Financial Institutions (Business Outsourcing Regulations), certain types of financial companies such as banks, insurance companies and credit card companies (collectively defined as 'financial institutions' for the purpose of this regulation), are permitted to outsource their business operations including data processing, except for instances:

- where the work includes 'essential elements' of the financial institution's business for which licensing is required (such 'essential elements' being exhaustively listed under the Business Outsourcing Regulations);
- where the relevant laws and regulations require the work to be performed by such financial institution; or
- where the outsourcing may significantly undermine the soundness or credibility of such financial institutions or cause extreme concerns of disorder in the financial system or damage to financial users.

Upon deciding to outsource work to a third party, these financial institutions must report this fact to the regulator at least seven business days before the outsourcing commences, unless exemptions under the Business Outsourcing Regulations apply.

Further, in the case of outsourcing data processing, specifically, the Regulations on Outsourcing of Data Processing of Financial Companies apply as special provisions over the Business Outsourcing Regulations. The Data Processing Outsourcing Regulations apply to 'financial companies' whose scope is more broadly defined than 'financial institutions' under the Business Outsourcing Regulations to include other types of financial service

providers such as electronic financial businesses and financial product advisory companies. These financial companies are permitted to outsource their data processing, except for instances where:

- relevant laws and regulations prescribe otherwise;
- the financial company has received a warning or a regulatory sanction with respect to user information in the past three years; or
- the outsourcing may significantly undermine the soundness or credibility of the financial company or cause extreme concerns of disorder in the financial system or damage to financial users.

In addition, financial companies may not outsource the processing of 'uniquely identifiable information' (namely, resident registration numbers, driver's licence numbers, passport numbers and alien registration numbers) to third parties located outside of South Korea. Upon deciding to outsource data processing to a third party, a financial company must report this fact to the regulator at least seven days before the outsourcing commences if the third party is a domestic company, or at least 30 days before the outsourcing commences if it is an offshore company.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

If a financial company processes a user's unique identification information or personal credit information through cloud computing services, the financial company's physical data processing system (namely, server) must be located in South Korea. However, if the financial company is a branch of a foreign financial company, such financial company may use a data processing system located outside of South Korea.

Additionally, financial companies are required to isolate and keep separate their internal work system connected to internal communication networks from external communication networks such as the internet or wireless network to prevent electronic intervention into their information processing system and information and communication network (the network separation rule). For financial companies using cloud computing services, it is necessary to have internal network separation functionality (eg, virtual private cloud or virtual network) in place to allocate a private internet protocol address and establish a logical network that is separate and isolated from the external communication network. If financial companies intend to use public web servers, they must be established in an independent cloud network that is separate from a cloud network dedicated to an internal work system.

Other measures that financial companies are required to implement to use cloud computing services include:

- to assess the soundness and stability of the information processing system based on internal criteria;
- to assess the soundness and stability of the cloud computing service provider (CSP);
- to establish and operate a work contingency plan and security-ensuring measures for the use of cloud computing services; and

- make periodical reporting about the use of cloud computing services in use to the Financial Supervisory Service.

Regulations for using a cloud system are being eased due to the recent revisions of the Financial Supervisory Regulations (1 January 2023) and the guidelines for cloud computing services in the financial sector (2 February 2023). The number of CSP evaluation items was reduced from 141 to 54. CSP evaluation standards suitable for SaaS were established. Financial companies that desire to use cloud computing services are now required to make regulatory reporting about the use of cloud computing services after adopting them (previously, pre-adoption reporting was required). In addition, the financial authorities announced that they will adopt exceptions to the network separation rule for the use of SaaS-type software through the sandbox system if the cloud computing service is not related to financial transactions and does not deal with customer transaction information.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

The source code of software is protected as copyrighted work under the Copyright Act if the creativity of expression is recognised and also as a trade secret under the Unfair Competition Prevention and Trade Secret Protection Act if it has been managed as a secret without being disclosed to the public and has an independent economic value. While registration is not necessary to have a copyright, without registration as copyright, it is not possible to assert copyright of a source code against a third party with regard to the transfer of the author's property right associated with the source code.

Meanwhile, an invention of a computer program method or business method can be protected as a patented invention if information processing by software on the computer is specifically realised by using hardware (Supreme Court Decision 2007Hu256 rendered on 24 December 2008).

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Under the Copyright Act, the employer acquires copyright as an author of the work made for hire (namely, a work made by an employee within the scope of his or her work duties) if it is published under the name of the employer, unless otherwise provided in the contract or employment rules. However, in the case of a computer program developed by an employee, the employer becomes an author regardless of whether the computer program is published under the name of the employer.

Meanwhile, under the Invention Promotion Act, if an invention of an employee, executive of a corporation or a public official created with respect to his or her duties has a nature of belonging to the scope of work of the corporation, state or local government employing the inventor and the act that led to the creation of the invention belongs to the present or previous work duties of an inventor, the inventor would acquire a patent, model utility and design rights for the invention. However, the employer may succeed in the rights granted to the inventors by way of the contract or employment regulations as long as it pays fair compensation to the inventor.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Except as otherwise agreed in writing, each joint owner of a patent may independently practice the patented invention without the consent of all other joint owners pursuant to the Patent Act. However, no joint owner may, without the consent of all other joint owners, assign his or her share of the patent or establish any pledge right over it, or grant a licence of the patent to a third party. This rule applies the same to design rights and trademark rights. Similarly, with respect to copyrights, an author's economic right to a joint work may not be licensed to a third party without the unanimous agreement of all the holders of the author's economic right, and no holder of the author's economic right shall be entitled to transfer by assignment or pledge his or her share of author's economic right without the consent of the other authors.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

For information to be protected as a trade secret, such information shall not be known publicly, have independent economic value and be managed as a secret.

The court may limit the access to parts of litigation records that contain secrets to the parties to protect trade secrets even during the course of litigation.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Branding can be protected under the Trademark Act. Trademark rights are established with registration with the South Korean Intellectual Property Office. A trademark holder holds the exclusive right to use his or her registered trademark in relation to designated goods.

The branding can also be protected without trademark registration if its emblem is widely known in South Korea. Therefore, if there is a branding intended to be used by fintech companies, they are advised to review whether the branding is identical or similar to

another branding that is already a registered trademark in South Korea, or another person's name, trade name, trademark, container or package of goods, or any other mark indicating another person's goods or business, to the extent to cause confusion with another person's goods, commercial facilities or activities.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

The holder of the infringed intellectual property rights may seek compensatory damage and injunctive relief (such as destruction of infringing objects or removal of facilities provided for infringement) as well as criminal punishment by filing a criminal complaint against the infringer.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

No. However, imposing less strict regulations on fintech companies compared to traditional financial institutions (eg, banks) subject to relatively stringent regulations under the existing laws has sparked a controversy over reverse discrimination against financial institutions amid the growing market presence of fintech companies.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

The South Korean government offers tax incentives for fintech companies and small- and medium-sized companies in South Korea. The tax incentives will apply to fintech businesses established in and after 2020.

In February 2020, the amended Enforcement Decree of the Special Tax Treatment Control Law included the following types of fintech companies as small- and medium-sized start-ups or venture companies entitled to receive 50 per cent income tax and corporate income tax relief for up to five years:

- electronic financial service providers under the Electronic Financial Transaction Act;
- online small-sized investment brokers under the Financial Investment Services and Capital Markets Act; and

Read this article on Lexology

- small-amount overseas remittance service providers under the Enforcement Decree of the Foreign Exchange Transactions Act.

Small- and medium-sized companies established in certain designated areas in South Korea, which are typically not located in highly populated cities, can receive a 50 per cent corporate income tax relief for up to five years on their business income.

Companies identified as 'venture businesses' by the South Korean government, which many fintech companies may qualify to be, may receive a 50 per cent corporate income tax relief for up to five years on their business income even if they are located in highly populated cities in South Korea.

Research and development (R&D) tax credits may also be available for specified R&D costs (including labour costs and material costs) that satisfy certain legal requirements, which may be relevant to fintech companies or small- and medium-sized companies with R&D activities.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

There are no recent tax law changes that could increase the tax burden on companies in the fintech industry.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

The Ministry of Justice has improved the system by establishing a new visa type to address labour shortages in high-tech industries.

Previously, foreign speciality worker visas were issued for only 93 occupations, but to proactively address new industries and occupations, a negative type of visa (E-7-S) was created, which may be issued to all high-tech professionals and high-income earners other than those that engage in designated industries relating to which issuance of the E-7-S visa is prohibited.

The E-7-S visa may be issued to:

1 prospective workers in high-tech industries who meet certain score requirements; and
2 high-income earners (GNI per capita of more than three times the previous year's GNI).

Regarding (1), the list of high-tech industries is determined and announced by the government and currently includes technology fields such as smart services, basic software computing, convergence software, and embedded software.

In addition, the number of skilled worker visas to be issued annually to alleviate labour shortages in the industry has been expanded, the requirements for specialised worker visas (E-7) have been relaxed, and the wage threshold for issuing visas to foreigners employed by small and medium-sized enterprises, ventures and non-metropolitan areas has also been relaxed.

There are also discussions about establishing an immigration agency that serves as a control tower to lead immigration policy work that is spread across various ministries to expand the economically active population.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

The proposed amendment to Electronic Financial Transactions Act (EFTA) passed the plenary meeting of the National Policy Committee of the National Assembly on 11 May 2023.

The proposal was brought to the table after the Merger Point incident of August 2021 and the increasing use of electronic payment means make it necessary to provide greater protection to the users of electronic prepayment means offered by Prepayment Service Providers. The proposal, among others, aims to expand the scope of electronic prepayment means (by abolishing the requirement that the scope of goods or services that can be purchased by 'two or more industries') and reduce the exemption from the registration requirement. It should be noted that a person who becomes subject to the registration due to the enforcement of the proposed amendments shall register within six months from the enforcement date (namely, one year after the promulgation).

Other key points of the proposal are as follows:

- to introduce rules of conduct to be complied with by any person who has its business registered to issue and manage electronic prepayment means (Prepayment Service Provider);
- to expand the scope of electronic prepayment means and strengthen the requirements for registration exemption;
- to manage prepaid charge amounts separately in a safe manner through the use of trust accounts or deposit accounts; and
- to designate a buy now, pay later (BNPL) service as a concurrent business under EFTA, instead of allowing an exception through the regulatory sandbox.

Further, the proposed amendments will impose restrictions on discount issuance creating refund obligations for refunds, businesses should prepare to take measures for compliance

with the regulations, such as preparation of internal control standards and amendment of their service terms.

Last, BNPL service providers will need to obtain service approval from the FSC. Also, since most of the details regarding the provision of the BNPL service to users, such as its scope, usage limit, total credit limit, management soundness control, credit information management, debt collection management plan and user protection plan, will be later set forth through the revised EFTA enforcement decree.

bkl BAE, KIM & LEE

Juho Yoon	juho.yoon@bkl.co.kr
Young Ju Park	youngju.park@bkl.co.kr
Se Yeong Im	seyeong.im@bkl.co.kr
Jinhee Rhew	jinhee.rhew@bkl.co.kr

Tower B Centropolis, 26 Ujeongguk-ro
Jongno-gu, Seoul 03161, South Korea
Tel: +82 2 3404 0000
www.bkl.co.kr

Read more from this firm on Lexology

Read this article on Lexology

Spain

Carmen Torres, Ignacio González, Juan Sosa, María Tomillo and Raquel Ballesteros*
Simmons & Simmons

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES	**505**
General innovation climate	505
Government and regulatory support	506
FINANCIAL REGULATION	**506**
Regulatory bodies	506
Regulated activities	507
Consumer lending	508
Secondary market loan trading	508
Collective investment schemes	508
Alternative investment funds	509
Peer-to-peer and marketplace lending	509
Crowdfunding	509
Invoice trading	510
Payment services	510
Open banking	511
Robo-advice	511
Insurance products	512
Credit references	512
CROSS-BORDER REGULATION	**512**
Passporting	512
Requirement for a local presence	512
SALES AND MARKETING	**513**
Restrictions	513
CRYPTOASSETS AND TOKENS	**514**
Distributed ledger technology	514
Cryptoassets	514
Token issuance	515
ARTIFICIAL INTELLIGENCE	**518**
Artificial intelligence	518
CHANGE OF CONTROL	**519**
Notification and consent	519
FINANCIAL CRIME	**519**

Read this article on Lexology

Anti-bribery and anti-money laundering procedures 519
Guidance 520

DATA PROTECTION AND CYBERSECURITY 520
Data protection 520
Cybersecurity 522

OUTSOURCING AND CLOUD COMPUTING 523
Outsourcing 523
Cloud computing 523

INTELLECTUAL PROPERTY RIGHTS 524
IP protection for software 524
IP developed by employees and contractors 525
Joint ownership 525
Trade secrets 526
Branding 526
Remedies for infringement of IP 527

COMPETITION 527
Sector-specific issues 527

TAX 527
Incentives 527
Increased tax burden 528

IMMIGRATION 528
Sector-specific schemes 528

UPDATE AND TRENDS 528
Current developments 528

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

The Spanish fintech community is one of the biggest in Europe. In this regard, Spain continues to promote this type of business, and the number of companies that use innovation and technology in the financial industry increases each year. There are studies that show that 70 per cent of the total number of fintech companies provide services linked to credit activities. The number of companies focused on electronic payments is increasing as well as those dedicated to investment solutions.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

The Spanish Securities Market Commission (CNMV) set up a point of contact for business initiatives related to financial innovations, which is currently available on the CNMV's online portal – the CNMV Fintech Portal. This site gives online support to promote fintech initiatives that deliver better outcomes for consumers and that improve the efficiency and competitiveness of the Spanish financial markets. Through this site, the CNMV collaborates with fintech businesses and financial institutions, providing guidance regarding the interpretation and application of rules and regulations where appropriate. Law No. 7/2020, of 13 November, for the digital transformation of the financial system regulates the fintech sandbox in Spain, following the models already established in other jurisdictions. Under this Law, among others, the following objectives have been met:

- financial sustainability control and risk minimisation;
- mitigation and adaptation of the regulatory burden;
- creation of a space to boost the development of open financial innovation; and
- the attraction of international investment.

This legislation offers new opportunities for this country and important advantages to improve the position of the Spanish fintech sector. Since the creation of the fintech sandbox for Spain, a significant number of projects have been submitted, and some of those initiatives have been already accepted and are being assessed (through a process in which the General Secretary of the Treasury in Spain and the relevant supervisory authorities in Spain – the Bank of Spain, CNMV and the General Directorate for Insurance and Pension Funds – actively participate). The objectives of the accepted initiatives are aligned with those indicated in the aforementioned Law No. 7/2020, and will contribute to promoting the digital transformation of the financial system, improving services to clients and the activity of supervisory authorities, generating significant potential gains for the different participants in this industry and society as a whole. The Spanish Association of Fintech and Insurtech actively participated in the creation of this fintech sandbox. The sandbox is designed to position Spain as a leader in financial innovation.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

The regulator in charge of supervision of fintech products and services is the Spanish Securities Market Commission (CNMV) together with the Bank of Spain and the General Directorate for Insurance and Pension Funds, depending on the type of entity intending to provide services in Spain and the exact nature of those services.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

There are a large number of activities that, when carried out in Spain on a professional and ongoing basis in respect of specified financial instruments, trigger licensing requirements. These are set out in a number of different regulations, including those implementing Directive 2014/65/EU (Markets in Financial Instruments Directive II) in Spain as well as legislation that governs activities carried out by financial institutions, such as credit entities.

The most common activities that may require a licence with respect to specified financial-instruments include:

- the reception and transmission of orders;
- the execution of orders on behalf of clients;
- portfolio management;
- providing investment advice (which requires that specific recommendations are made as opposed to providing generic advice only);
- the underwriting or placing of financial instruments, or both;
- dealing in investments as the principal or agent;
- arranging or bringing about deals in investments; and
- making arrangements with a view to transactions in investments.

To carry on any of these activities in relation to specified financial instruments on a professional and ongoing basis in Spain, the relevant entity or natural person must obtain the appropriate authorisation or passport. In addition to this authorisation, registration is a requirement to operate in Spain. Authorisation is also required to carry out marketing or canvassing of clients on a professional basis, as well as prior or preliminary activities related to investment services and the offering of financial instruments.

A similar regime applies to the provision of services that are typical activities carried out by credit entities. The Spanish implementing text of Directive 2013/36/EU (Capital Requirements Directive) expressly states that the activity of taking repayable funds from the public (whether in the form of deposits, loans or temporary transfers of financial assets or other analogous actions) is a licensable activity that can only be carried out by credit entities that are authorised to operate in Spain and duly registered with the Bank of Spain. Taking repayable funds from the public using capital markets through the issuance and placement of instruments with the aim of giving credit is a reserved activity.

Notably, the provision of loans does not trigger licensing requirements, even though it is a typical activity of credit entities. However, while the activity of extending credit is not a reserved activity, it is usually connected to other regulated activities that trigger licensing requirements.

Regarding payment services, it is prohibited for entities or natural persons who are not payment service providers (apart from certain exceptions derived from Directive (EU) 2015/2366

(Second Payment Services Directive) (PSD2) to provide payment services in Spain on a professional basis.

Consumer lending

5 Is consumer lending regulated in your jurisdiction?

Although it has traditionally been an activity carried out in Spain by credit institutions and financial credit establishments, in the case of a non-financial institution (namely, neither a credit institution nor a financial credit establishment) that is dedicated solely to the activity of granting consumer loans, this non-credit institution (formed as a company) may carry out this activity without a licence. The number of persons who tend to get credit from non-financial institutions offering personal loans rather than other traditional means (eg, banking credit cards and banking loans) is increasing.

The regulatory regime for consumer credit is governed by Law No. 16/2011, of 24 June, on Credit Agreements for Consumers. This regulatory regime applies to all contracts where entities or natural persons in the course of their business activity, profession or craft, grant or promise to grant a consumer credit in the form of a deferred payment, loan, opening credit or any other equivalent means of financing, with the aim of covering personal needs outside of his or her professional or business activity and amounting to at least €200. This regulation broadly sets out the requirements that lenders need to comply with in relation to the provision of information, documents and statements, and the detailed requirements as to the form and content of the credit agreement itself, including advertising, information to consumers, content, form of the contracts, cases of null-and-void contracts, right of withdrawal and costs.

In addition, Legislative Decree 1/2007, of 16 November, for the Protection of Consumers and Users also applies to consumer lending. Depending on the circumstances, other Spanish supplementary regulations may also be relevant.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

Provided that the loan itself is being traded, and not the loan instrument (the financial instrument creating or acknowledging indebtedness), there are no restrictions on trading loans in the secondary market.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

The general regulatory regime for collective investment schemes (CISs) in Spain consists of the transposition of Directive 2009/65/EC (Undertakings for Collective Investment in Transferable Securities Directive) and Directive 2011/61/EU (Alternative Investment

Fund Managers Directive) (AIFMD), in addition to the regime that applies specifically to Spanish CISs.

CISs are regulated products in Spain and must be locally registered. Management and distribution of CISs (namely, marketing, promotion and advertising) may only be carried out by licensed entities in Spain as these activities trigger licensing requirements. Marketing of CISs is defined as those activities aimed at raising funds from clients by way of any advertising activity for their investment into the CIS. Advertising activity consists of targeting the public through telephone calls initiated by the CIS or its management company, home visits, personalised letters, emails or any other electronic media forming part of a dissemination, promotional or marketing campaign.

Whether a fintech company falls within the scope of this regulatory regime will depend on the exact nature of its business and the type of activities being carried out.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

Managers of alternative investment funds are regulated in Spain under the AIFMD, which was implemented in Spain by Law No. 22/2014, of 12 November, governing private equity entities, other closed-ended collective investment undertakings, and the management companies of closed-ended collective investment undertakings, which amended Law No. 35/2003, of 4 November, on Collective Investment Schemes.

Peer-to-peer and marketplace lending

9 | Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Peer-to-peer lending is considered a crowd-lending activity under Spanish legislation and is regulated by Law No. 5/2015, of 27 April, on the Promotion of Business Financing.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

Crowdfunding is regulated by Law No. 5/2015, of 27 April, on the Promotion of Business Financing. This Law affects reward-based crowdfunding, equity crowdfunding and crowd lending, and governs, among others, the normal operating model and regime of platforms, the accreditation of the investor and the limits established for the amount of the investment. These limits, which are some of the most restrictive elements established in the Law, include limitations on:

- raising funds for start-ups that amount to €5 million for accredited investors (namely, professional investors) and €2 million for non-accredited investors;
- equity crowdfunding projects, which cannot exceed 125 per cent of the project's projected target; and

Read this article on Lexology

- platforms and projects to be invested in by non-accredited investors, which are capped at €10,000 and €3,000 respectively.

It is expressly established that these types of investments are not covered by the guarantee fund.

Additionally, Regulation (EU) 2020/1503 on European crowdfunding service providers for business, which regulates and tries to harmonise the functioning of these alternative financing systems, entered into force on 10 November 2021.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

There is no specific regulation of invoice trading in Spain. As a general rule, there are no restrictions on invoice trading; however, the activities and structure of a firm engaged in invoice trading should be analysed to determine whether a regulated activity that requires permission or authorisation is taking place.

Payment services

12 | Are payment services regulated in your jurisdiction?

Payment services are regulated by Royal Decree-Law No. 736/2019, of 20 December, on the legal regime on payment services and payment entities, which completes the transposition of PSD2 in Spain, which was partially implemented by means of the Royal Decree-Law No. 19/2018, of 23 November, on payment services and other financial measures.

Payment services include:

- services enabling cash to be placed on a payment account, as well as all the operations required for operating a payment account;
- services enabling cash withdrawals from a payment account, as well as all the operations required for operating a payment account;
- execution of payment transactions;
- transfers of funds on a payment account with the user's payment service provider or with another payment service provider;
- execution of payment transactions where the funds are covered by a credit line for a payment service user;
- issuing and acquiring payment instruments;
- money remittance; and
- execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and a payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.

To provide payment services in Spain, a firm must fall within the definition of a 'payment service provider', which includes:

- credit institutions;
- electronic money institutions;
- the national postal service of Spain;
- the Bank of Spain; and
- the Spanish general government administration, autonomous communities and local bodies.

A firm that provides payment services in or from Spain as a regular occupation or business activity (and is not exempt) must apply for registration as a payment institution. Sanctions may be imposed on any natural or legal person providing payment services without authorisation. Since December 2019, entities wishing to act as payment institutions must follow the specific procedure established under aforementioned Royal Decree-Law No. 736/2019, of 20 December, and submit a request with the Bank of Spain to obtain relevant authorisation. The cross-border business of payment institutions will be possible in Spain as far as relevant passports to set up a local branch or agents have been received by the Bank of Spain from entities located within the territory of the European Union. The provision of services without the presence of these entities in Spain will be also available if relevant notifications are received by the Bank of Spain. Spanish entities will provide services abroad if the Bank of Spain has received relevant notifications. In the case of the provision of activities in or from entities located out of the European Union, express authorisation is needed. In certain cases, the Bank of Spain may reject this authorisation.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

No.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

There is no specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in Spain. In terms of licensing requirements, Spanish legislation does not distinguish based on the profiles of targeted investors, whether professional or retail. Automated access to investment products through fintech companies in Spain is only possible if the relevant licences are duly obtained. Fintech companies may provide automated activities related to investment advice (when referring to specific financial instruments taking into account the personal circumstance of the investor) and portfolio management in Spain, but these activities imply the provision of certain services that trigger licensing requirements. In any case, authorisation and registration with the CNMV will be mandatory. In Spain, there are a number of entities providing this type of service, most of them being investment firms exclusively dedicated to providing investment advice.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Selling or marketing insurance products in Spain is a regulated activity and entities providing this service fall under the relevant Spanish regulation. In this regard, a fintech company must act under the form of a regulated entity (eg, insurance company or insurance intermediary as broker or agent). The Association of Fintech and Insurtech has published a white paper on fintech regulation in Spain, aimed at creating an adequate framework for these types of entities and to encourage alternatives to the existing Spanish regulations for financial services providers in Spain, including insurance services providers.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

The rules on credit ratings laid down in Regulation (EC) No. 1060/2009 (as amended) apply in Spain. A credit-rating agency is required to adopt, implement and enforce adequate measures to ensure that its credit ratings are based on a thorough analysis of all the information that is available and that is relevant to its analysis according to its rating methodologies. At present, there are only two credit-rating agencies domiciled in Spain and included in the official register of the CNMV.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

An EEA firm may exercise passport rights to provide services in Spain and may provide services through a local branch or agent or on a cross-border basis without a presence in the territory. A non-EEA firm or an EEA firm that is not undertaking an activity that can be passported into Spain must establish a local presence, obtain an appropriate licence or, in some cases, receive authorisation from the relevant regulator to operate on a cross-border basis.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

An EEA firm may exercise passport rights to provide services in Spain. A non-EEA firm or an EEA firm that is not undertaking an activity that can be passported into Spain must establish a local presence, obtain an appropriate licence or, in some cases, receive authorisation from the relevant regulator to operate on a cross-border basis.

Read this article on Lexology

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Although general rules on marketing and advertising shall apply to the investment business, there are specific regulations covering the sales and marketing of investment services and products in Spain. In accordance with Law No. 6/2023, of 17 March 2023, on Securities Markets and Investment Services (the Securities Market Law), this activity must be only carried out by entities that are authorised or passported to provide the relevant investment service.

Although the sales and marketing of financial services is not an investment service itself, the activity consisting of marketing as well as the canvassing of clients triggers licensing requirements in Spain.

Advertising and marketing of investment services and products are covered under sectorial regulations, in particular, under Order EHA/1717/2010, of 11 June, on Regulation and Control of Advertising of Investment Services and Products and Spanish Securities Market Commission (CNMV) Circular 2/2020, of 28 October, on advertising of investment products and services that cover this type of advertising in Spain and include a definition of advertising activity. In this regard, advertising activity includes a communication to the general public aimed to promote, directly or indirectly through third parties, the contracting of a specific investment service or product (covering financial instruments under Directive 2014/65/EU (Markets in Financial Instruments Directive II)), as well as those communications made in the course of a public offer with the aim of impacting its result. It is expressly contemplated that advertising activity shall exist in respect of communications to the general public on the management or marketing of collective investment schemes, private equity schemes or securitisation vehicles, although these communications do not refer to a specific product. This legal provision determines the procedures and controls that entities must have in place when producing advertising materials in connection with investment services and products.

The content of the advertising material in no case may contradict or play down the importance of the information contained in the prospectus and the key investor information document. Advertising materials must be clearly recognisable as such and the promotional character of the message must be explicit and evident. All information included in the materials must be fair, clear and not misleading, with the ultimate goal of abiding by the general obligation to act in an honest, loyal and professional manner and in the best interests of clients while rendering investment services.

The CNMV has supervisory functions in respect of the marketing and advertising of investment services and products.

Banking

In respect of banking activities, on 15 July 2020, Circular 4/2020, of 26 June, of the Bank of Spain, on advertising of banking products and services (Bank of Spain Circular 4/2020) was

published. Bank of Spain Circular 4/2020 repealed Circular 6/2010, of 28 September, of the Bank of Spain, on advertising of banking products and services and it develops Ministerial Order EHA/1718/2010, of 11 June, on regulation and control of advertising related to banking services and products (Order 1718/2010). Other rules such as Order EHA/2899/2011, of 28 October, on Transparency and Protection of Clients of Banking Services may also apply.

Bank of Spain Circular 4/2020, Order 1718/2010, CNMV Circular 2/2020 and Order EHA 1717/2010 together with Law No. 10/2014, of 26 June, on management, supervision and solvency of credit institutions (Law No. 10/2014) and implementing regulations, and the Securities Market Law and its implementing regulations fully complete the sectorial legislation on advertising of banking and investment products and services Spain, with the general rules on advertising that continue to be governed by General Law No. 34/1988, of November 11, on Advertising (Law No. 34/1988). The Spanish regulation governing the advertising of banking products and services and the one governing the advertising of investment products and services follow the same pattern.

Bank of Spain Circular 4/2020 and CNMV Circular 2/2020 contain rules on controls and procedures that credit institutions must adopt when they are promoting their products in Spain, their potential adhesion to self-regulation systems, and the content and format of such promotions including information on the supervisory powers of the Bank of Spain and the CNMV and potential sanctions that may be enforced (eg, cessation or rectification of certain promotional activities).

The Bank of Spain has supervisory functions in respect of the marketing and advertising of banking services and products.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

No.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

On 29 April 2021, Royal Decree-Law No. 7/2021 entered into force, implementing Directive (EU) 2018/843 (Fifth Anti-Money Laundering Directive) and amending certain provisions of Law No. 10/2010 on the prevention of money laundering and terrorist financing. The Law includes regulation of the information to be disclosed by service providers of digital currency exchange, transfer of digital currency and custody of digital currency, among others.

The Law considers service providers as subject to the Spanish anti-money laundering legislation. Cryptoasset service providers must be included in the relevant register at the Bank of Spain. They have nine months from the entry into force of Royal Decree-Law No. 7/2021 to be included in the relevant register. Breach of the registration obligation and the provision of these services to Spanish residents would be qualified as a very serious infringement.

The new registration requirement before the Bank of Spain was published on 20 October 2021.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

The Spanish Securities Market Commission (CNMV) and the Bank of Spain published a joint statement on 9 February 2021, building on another statement from 2018, in which they warned about the risks that these new types of assets pose for participants in the financial system and, in particular, for small investors. The statement highlighted the complexity, volatility and potential lack of liquidity of these investments.

Royal Decree-Law No. 5/2021, of 12 March, on extraordinary measures to support business solvency in response to the covid-19 pandemic, introduced a new article 240-bis in Law No. 6/2023, of 17 March 2023, on Securities Markets and Investment Services (the Securities Market Law) to strengthen the legal framework for the protection of investors with regard to the advertising of new instruments and financial assets in the digital area.

The amendment of the Securities Market Law has regulated that the CNMV has been granted powers to subject the advertising of cryptoassets, and other assets and instruments that are not regulated by the Securities Law and that are offered as investments, to administrative control.

On 10 January 2022, CNMV Circular 1/2022 of 10 January, on the advertising of cryptoassets presented as a means of investment (CNMV Circular 1/2022), was published. It aims to develop the rules, principles and criteria to which the advertising of cryptoassets shall be subject, in particular, to delimit the scope of application and obliged entities to CNMV Circular 1/2022.

CNMV Circular 1/2022 governs the advertising of cryptoassets that are the means of investment. For these purposes, any advertising directed at investors or potential investors in Spain that, implicitly or explicitly, offers or draws attention to cryptoassets as a means of investment will be considered to be advertising activity.

In all circumstances, it will be presumed that a cryptoasset is offered or attention is drawn to it as a possible means of investment when its acquisition is promoted or any reference to its return, price or value, current or future is made, which might suggest an opportunity to invest in such cryptoasset, even though it may occasionally be used as a means of exchange.

Likewise, in all circumstances, advertising will be understood to be aimed at investors in Spain when it is provided on physical media in Spain, through Spanish media (including web

pages or domains) and when it is provided in Spanish or other official languages, unless it contains a statement that the services or products offered are not aimed at or accessible to investors in Spain.

CNMV Circular 1/2022 will be applicable to the following parties:

- cryptoasset service providers when they engage in cryptoasset advertising activities;
- advertising service providers; and
- any natural or legal person, other than those indicated in previous points, who on their own initiative or on behalf of third parties, engages in an activity of advertising of cryptoassets.

When designing their advertising campaigns and each of the advertising pieces that comprise them, obliged entities to CNMV Circular 1/2022 shall take into account the nature and complexity of the advertised product, the characteristics of the communications media used and the target audience.

All commercial communications must include information on the risks of the product they advertise, specifically:

- The following warning shall be included in the commercial communication, using a format and positioning that ensures its relevance in the advertising piece and not as secondary information or as a footnote: 'Investment in cryptoassets is unregulated, may not be suitable for retail investors and the entire amount invested may be lost.'
- A link or reference to the location of the additional information shall be included, which shall, as a minimum, refer to the information and risks identified. The link must be identified with the following text: 'It is important to read and understand the risks of this investment, which are explained in detail on this site.'
- When the medium used only allows for a reference, an indication must be given of where information about the risks can be found and the importance of reading that information.

Advertising activity aimed at investors in Spain shall not require prior CNMV notification, except in the case of mass advertising campaigns. However, even when they are not mass advertising campaigns in the strictest sense, some obliged entities to CNMV Circular 2/2022 may be required to provide prior notification for all their advertising campaigns, where it is considered necessary due to the potential impact on their target audience.

In the exercise of its supervisory function, the CNMV can ask the obliged entities to CNMV Circular 1/2022 to provide specific information on advertising campaigns or pieces to assess their compliance with the requirements set forth in CNMV Circular 1/2022. This type of request must be answered by the entity within a period of three business days.

The obliged entities to CNMV Circular 2/2022 shall keep a register of the following information and documentation relating to ongoing advertising campaigns and those carried out in the past two years:

- General information on the campaign: start and end date, territorial scope, description of the target audience, list of the media and advertising channels used for dissemination and a quantitative estimate of the number of people to which it is being targeted.

Read this article on Lexology

- Specific information on the advertising pieces: a copy must be kept of all advertising pieces with a different message (including clarifications or legal warnings) or format (radio spot, television advertisement, banner, poster, etc) broadcast during the campaign, in the original format or in electronic format that can be accessed.
- Identification of the advertising service providers and the advertising contracts or agreements entered into.

Obliged entities to CNMV Circular 2/2022 that carry out mass advertising campaigns must provide the documentation and information indicated in CNMV Circular 2/2022 at least 10 business days before their execution.

They must present a document giving prior notification of the mass advertising campaign that shall adhere to the template included for this purpose on the CNMV's website, in addition to the following documentation, which shall be clear, concise, consistent and sufficient to allow an assessment to be made of the scope and impact it may have on the public:

- General information about the campaign: details of the cryptoassets that are the object of the campaign or the services to be advertised, a description of the target audience and a list of the media and advertising media used for their dissemination.
- Specific information on the advertising pieces: a copy of all advertising pieces with a different message (including clarifications or legal warnings and warnings about risks) or format (radio spot, television advertisement, banner, poster, etc) to be broadcast during the campaign, in the original format or in an electronic format that can be read or accessed.

The prior notification will allow the advertising campaign to start 10 business days after its presentation, unless the CNMV indicates otherwise. Under no circumstances shall a lack of response from the CNMV during the period between the notification and the start of the campaign imply that the CNMV considers that the campaign complies with all the rules contained in CNMV Circular 1/2022.

Further, in September 2020, the European Commission made a proposal for the regulation of markets in crypto-assets (MiCA) (the MiCA Proposal). This regulation intends to cover and regulate those cryptoassets that are not regulated by the current regulation in force (an example of a regulated cryptoasset would be electronic money). However, a large part of the cryptoassets typology is not framed within said regulation.

In this sense, the MiCA Proposal aims to harmonise the entire legal regime within the scope of currently unregulated cryptoassets; thus, all national regulations on any matter within its scope of application would be voided, based on the principle of the primacy of EU law.

An additional purpose of the MiCA Proposal is to guarantee an appropriate legal framework for the promotion of innovation and new technologies guaranteeing investor protection.

Finally, it should be noted that the proposed regulation will apply to all providers who:

- issue or advise on the issuance of cryptoassets; and
- provide cryptoassets services within the European Union.

Read this article on Lexology

Some cryptoassets are considered electronic money (eg, stablecoins), and these will not be regulated by the MiCA Proposal.

Although there are no local regulations governing this type of product in Spain, the CNMV and Bank of Spain have expressed their concern on multiple occasions regarding the risks involved when dealing with this type of product. In this regard, the last publication was a joint press statement by the CNMV and the Bank of Spain on cryptocurrency investment risks. Following joint press statements published in 2018 and 2021, where the Bank of Spain and the CNMV warned about the high risk posed by these types of investments owing to, among other factors, their extreme volatility, complexity and lack of transparency, now both supervisory authorities in Spain include express alerts to the public on the fact that these products are complex instruments that may not be appropriate for small-scale savers, their price having a high speculative component that may even entail the loss of the amounts invested. Other aspects have been a matter of concern, such as the existence of leverage-derivative products linked to cryptocurrencies through which it is possible to indirectly invest in those instruments, and the risks linked to the use of cryptocurrencies as means of payment, among others.

On 14 March 2022, the Committee on Economic and Monetary Affairs of the European Parliament approved a new draft of the regulation on MiCA. In the approved draft, it has been agreed not to include the amendment that de facto prohibited the provision of services related to cryptoassets that were not environmentally friendly. This prohibition affected those that are mined with the proof of work mechanism.

Finally, the European Parliament has approved the final text of MiCA on 20 April 2023. The entry into force will be 20 days later than its publication. The version adopted by the European Parliament will have to be formally approved by the Council and will enter into force 20 days after its publication in the Official Journal of the European Union.

The MiCA Regulation will be applicable 18 months after the date of entry into force, with the exception of Titles III and IV (issuance of e-money tokens and asset-backed tokens), which will apply 12 months after the date of entry into force.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

The Spanish Securities Market Commission (CNMV) has stated that the fact that investment advice or portfolio management is automated does not make a difference in the way that the service is regulated and that the relevant conduct of business rules, suitability assessments and other rules apply in the normal way. In this regard, there are no specific rules or regulations governing the use of artificial intelligence.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

There are specific rules relating to the change of control of regulated entities. Where a person (whether acting separately or with others) decides to acquire, directly or indirectly, shares in a credit institution, insurance company or investment firm that imply acquiring a significant holding or taking control of the entity, the relevant regulators (the Bank of Spain, the Spanish Securities Market Commission or the General Directorate for Insurance and Pension Funds) must first be notified and provide their consent. The notification must be accompanied by documents and information that will enable the relevant regulator to analyse the suitability of the potential acquirer. Once the relevant regulator expressly states that there are no grounds to prevent the acquisition, the acquisition may take place.

A prior request must always be sent to the relevant supervisory authority and the acquisition may not take place before receiving relevant authorisations. There are specific procedures and standardised forms that must be used in these circumstances.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

There is no specific legal or regulatory requirement for fintech companies to have anti-money laundering procedures. The Spanish Anti-Money Laundering Law applies to a number of regulated entities and persons carrying out certain activities. Compliance with the Anti-Money Laundering Law is compulsory and includes an obligation to have appropriate policies and procedures in place to combat money laundering and terrorism financing.

Spanish legislation does not regulate anti-bribery and corruption separately. The relevant regulation establishes monitoring mechanisms to avoid illicit activity in organisations while also providing a range of sanctions, including the suspension of the activities and the dissolution of the company engaged in illegal activities. Regardless of whether they are regulated, fintech companies should adopt a proactive position to establish preventive criminal monitoring measures and appropriate policies and procedures as a matter of good governance and risk management.

Where initial coin offerings fall under the classification of a public offer, procedures to combat bribery or money laundering should be in place.

In May 2018, the EU approved new anti-money laundering legislation targeting anonymity in the cryptocurrency market.

Read this article on Lexology

On 29 April 2021, Royal Decree-Law No. 7/2021 entered into force, amending Spanish Law No. 10/2010 on the prevention of money laundering and terrorist financing and implementing Directive (EU) 2018/843 (Fifth Anti-Money Laundering Directive). The following developments shall be taken into account:

- new obliged entities:
    - virtual currency service providers for the exchange of fiat currencies and the custody of electronic wallets for these virtual currencies;
    - entities providing account information services (commonly known as 'aggregators'); and
    - insurance companies authorised to operate investment-related insurance business (amendment, not a new category); and
- creation of a central and single registry of beneficial ownership throughout the national territory of Spain; and
- creation of a registry of virtual currency providers.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no anti-financial crime guidance specifically for fintech firms. However, firms that are subject to the Anti-Money Laundering Law for carrying out certain types of activities subject to anti-money laundering checks should comply with it. In addition, these entities should follow the general recommendations for internal monitoring to prevent money laundering and terrorism financing issued by the Spanish Executive Service of the Commission for the Prevention of Money Laundering.

Regulatory and financial crime rules apply as far as the entities are subject to these regulations considering the type of activity or the type of entity (banks, insurance companies, asset managers, investment firms, etc). In this regard, there is an initiative proposing the creation of a specific regulatory framework for the fintech sector.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

On 25 May 2018, Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR) came into force with direct effect across the entire European Union. In Spain, additionally, domestic law (Organic Law No. 3/2018, of 5 December, on the protection of personal data and guarantee of digital rights (SLDP) was enacted and came into effect on 7 December 2018. Likewise, among other 'domestic peripheric regulations', two of them that play an important role in the field of processing personal data within the fintech sector, Law No. 34/2002,

of July 11, on services of the information society and electronic commerce (LSSIyCE) and General Telecommunications Law No. 11/2022, of June 28, which transposes Directive 2002/58/EC, of July 12, on privacy and electronic communications.

Within the European Union, the GDPR – given its direct and primacy effects – governs the processing of personal data provided that the material and territorial scope stated in article 2 and article 3 of the GDPR, respectively, is triggered. Likewise, the SLDP has regulated some outstanding key legal points from the GDPR and additionally has extended its approach to some other topics (among others):

- the appointment of the Spanish Data Protection Authority (AEPD) as the Spanish supervisory authority;
- granting powers of inspection and corrective measures to the AEPD;
- list of infringements, penalties and the particularities of the sanctioning procedure in place; and
- catalogue of new digital rights for the data subjects (seen from the other side, duties for the businesses).

The GDPR relies on general principles stated in article 5, 'accountability' presumably being the most disruptive one in comparison with the previous regime (Directive 95/46/EC (Data Protection Directive). The GDPR requires that any processing of personal data shall be done on a lawful basis, depending on the category of personal data (either general or standard (article 6) or special (article 9 in relation to article 6)). Additionally to the lawful basis, the GDPR requires a mandatory obligation to process personal data: to inform the data subject in the terms laid down in the GDPR. Such duty places a significant burden on businesses, as they shall always ensure that their customers are duly informed, which is a crucial change to the previous data protection regime.

The GPDR poses a significantly increased compliance burden on businesses (accountability principle), including, for example, mandatory requirements to notify the AEPD of data breaches; introduction of a new 'public body' named the 'Lead Supervisory Authority' aimed at exercising powers with regard to cross-border processing of personal data; and requirements for most private entities to appoint a data protection officer. Businesses that infringe the GDPR may be subject to a variety of corrective measures imposed by the supervisory authorities, among others, administrative fines of an amount up to €20 million or 4 per cent of global turnover, whichever is higher (eg, the last administrative fine imposed by the AEPD to Google LLC amounted to some €10 million).

Cross-border processing of data falls under the legal framework of the GDPR, therefore no relevant changes have to be borne in mind (except that the new public body, the Lead Supervisory Authority, will take on powers regarding cross-border processing of personal data).

International transfer of personal data to third countries (not including Iceland, Liechtenstein and Norway, as they are part of the European Economic Area) is covered by article 45(1) of the GDPR (transfers on the basis of an adequacy decision):

> *A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more*

specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

Note that the judgment of the Court of Justice of the European Union in *Schrems II*, handed down on 23 July 2020, annulled the 'privacy shield' that provided the legal framework (adequacy decision) for the international transfer of personal data between the European Union and the United States. As of today, there is no adequacy decision in place with the United States and due to the last non-binding opinions by the European Data Protection Board and the European Parliament's Committee on Civil Liberties, Justice and Home Affairs advising against the adequacy decision, we cannot expect an agreement between both parties in the coming months. The judgment also emphasised the responsibilities of exporters and importers to ensure that the processing of personal data has been and will continue to be carried out in compliance with the level of protection set by the GDPR. Additionally, to suspend the transfer or terminate the contract where the importer of the data is not, or is no longer, able to comply with standard data protection clauses incorporated in the relevant contract between exporter and importer. Whatever mechanism is chosen for the international transfer of personal data, it must be ensured that, overall, the transferred personal data will have the benefit of an essentially equivalent level of protection as in the European Union.

Likewise, in relation to the United Kingdom, it is important to mention that on 28 June 2021, the European Commission adopted an adequacy decision with the United Kingdom, which ensures the free flow of personal data between the two parties for a period of four years (until June 2025) (article 46 of the GDPR (transfers subject to appropriate safeguards) and article 49 of the GDPR (derogations for specific situations).

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

There are no local rules on cybersecurity for fintech companies, although Directive (EU) 2016/1148 on cybersecurity has been transposed by means of Royal Decree-Law No. 12/2018, of 7 September, which was amended by Royal Decree-Law No. 43/2021, of 26 January.

With regard to sector standards, public body the National Institute of Cybersecurity is in charge of cybersecurity issues and plays an important role in informing, advising and guiding private entities in relation to cybersecurity incidents. A brief guide on the fintech sector has been released on the Institute's website.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

There are no regulations specific to the outsourcing of IT systems, including in relation to cloud computing and the internet of things. However, depending on the activities contemplated, consideration will need to be given to the processing of personal data under Regulation (EU) 2016/679 (General Data Protection Regulation) and Organic Law No. 3/2018, of 5 December, on the protection of personal data and guarantee of digital rights' legal framework, aspects of the Intellectual Property Law approved by Royal Legislative Decree No. 1/1996, of 12 April (the Copyright Law), and parts of the General Telecommunications Law No. 9/2014, of 9 May.

Financial services companies planning to outsource certain services or activities may be subject to specific regulations. In general, credit institutions may delegate the provision of certain services and the carrying on of certain functions to a third party, provided that:

- there is no resulting void in the credit institution's functions or reduction in its internal control capacities; and
- supervisory authorities can continue to perform their supervisory responsibilities.

Note that outsourcing does not reduce a credit institution's liability for its legal obligations.

Additional restrictions apply to the delegation by a credit institution of essential services or essential functions. Generally, a service or function is considered essential if it could affect compliance with the terms of a credit institution's authorisation, financial results, solvency or the continuity of banking activity. Financial institutions must notify any agreements delegating essential services or functions to the Bank of Spain, the Spanish Securities Market Commission, or both, with one month's advance notice.

Bank of Spain Circular 2/2016 sets out further details regarding the extent to which outsourcing is permitted.

Credit institutions providing investment services must comply with additional requirements set out in Law No. 6/2023, of 17 March 2023, on Securities Markets and Investment Services (the Securities Market Law).

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

The EU Agency for Network and Information Security (ENISA) guidance titled 'Secure Use of Cloud Computing in the Finance Sector' contains analysis of the security of cloud computing systems in the finance sector and provides recommendations. Cooperation between

financial institutions, national financial supervisory authorities and cloud service providers is encouraged. ENISA advocates a risk-based approach to developing cloud computing systems in the finance sector.

Likewise, any storage of personal data provided through cloud computing services should bear in mind the processing of personal data (security measures adopted, international transfer of personal data, etc).

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Computer programs are protected, generally, as literary works under Royal Legislative Decree No. 1/1996, of 12 April (the Copyright Law). Although registration is not required for protection, it is highly recommended.

In the labour field, subject to the Copyright Law, software is generally considered a 'collective literary work', which entitles businesses to become the exclusive holder of moral and exploitation rights derived from the creation of the software. Nonetheless, even though such legal provision generally applies it is highly recommended to introduce in the employment contract clauses of assignment of exploitation rights in favour of the business.

Besides the labour field, which is caught by specific rules given the relationship between employer and employee, the two main ways of obtaining moral and exploitation rights derived from software are:

1 creation (original owner); or
2 assignment or license of exploitation rights (derivative owner)

In (2), the original creator will keep the moral rights as such rights cannot be assigned or licensed under the Copyright Law.

In some particular cases, software can be protected under a patent legal framework as long as it is considered a computer-implemented invention that solves a technical problem in an inventive way. In this regard, on 1 June 2023, the Agreement on a Unified Patent Court (UPC) came into force in 17 EU member states, excluding Spain due to its ratification rejection. However, the UPC Agreement leaves the door open to the rest of the EU member states, including Spain, to apply for accession to the European Unitary Patent system.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

As a general rule that applies to both IP (eg, patents) and copyright (eg, software), the exploitation rights of inventions or works created by employees:

- during the course of his or her role in the company; and
- related to the functions assigned to his or her job belongs to the employer, provided that the employer uses it for the business.

Nonetheless, there are particular exceptions stated in Spanish legislation (eg, the Patent Law) that would require analysis on a case-by-case basis. As a matter of recommendation, it is always advisable to introduce, in the employment contract, the assignment of exploitation right clauses in favour of the employer.

Contractors or consultants, as external to the entity, shall be required to assign or license the exploitation rights derived from the inter partes relationship, when acting as service providers. An ad hoc IP and copyright clause to set forth the legal regime applicable to the contract is highly recommended.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

In the field of IP (eg, see the Spanish Patent Law), the joint ownership of the patent exploitation right is expressly laid down and some specific rules apply. The first regime governing joint ownership is the agreement between the joint owners, which will not impede each joint owner from exploiting the patent; subsidiarily, the terms laid down in the Patent Law will apply; failing that, Spanish civil law principles will be triggered.

The Copyright Law differentiates between collaborative works and collective works. The first is made by the collaboration of different co-authors and its division must be agreed by all the co-authors, although no author can unreasonably withhold his or her consent for any exploitation once work has been released. Each co-author is able to exploit his or her part of the work unless it prejudices the work (as a whole). The collective work is made by different authors but under the initiative and coordination of a person or entity (normally, the second one), being the one in charge of the initiative and coordination task which will hold the exclusive morale and exploitation rights of the work.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Directive (EU) 2016/943 (Trade Secrets Directive) has been implemented in Spain by means of Law No. 1/2019, of 20 February, on trade secrets (the Trade Secret Law). Therefore, to benefit from trade secret protection three requisites shall be met (namely, confidential, business value by virtue of its secrecy and adequate measures implemented to keep it confidential).

Despite this, the lack of compliance with the requirements for trade secret protection does not mean a lack of protection, as there might be protection under the umbrella of 'know-how'. Commission Regulation (EU) No. 316/2014, of 21 March, defines 'know-how' as:

- a secret;
- substantial; and
- an identified package of practical information, resulting from experience and testing, without requiring proactive measures to be taken to ensure secrecy (as is required for trade secrets).

According to the Trade Secret Law, trade secrets' ownership cannot be alleged as an exception to disclose it before administrative bodies and judicial proceedings when they are performing their respective public duties, nonetheless effective and adequate measures shall be put in place to avoid the disclosure of trade secrets to third parties.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

In general terms, trademarks can be protected as registered trademarks either in Spain alone (as a Spanish trademark before the Spanish Patent and Trademark Office (OEPM), across the European Union (as an EU trademark before the European Union Intellectual Property Office (EUIPO) or throughout the international trademark procedure before the World Intellectual Property Office (WIPO). Certain branding, such as logos and stylised marks, can also be protected by the 'commercial name' legal regime, design rights and the requisites to be protected by copyright as artistic works may also be met.

The OEPM has a database that can be searched to identify which trademarks are already registered. In addition, the EUIPO trademark database can be searched to identify registered or applied for trademark rights with effect in the entire European Union. Likewise, the WIPO has an open global trademark database with information concerning national, EU and international trademark registrations.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

There are plenty of remedies related to IP and copyright infringements that may be of use to an injured party.

Regarding IP, the injured party is entitled, among others, to take measures before local or European offices (eg, see in the field of trademarks through annulment action or expiry due to lack of use action), file preventive letters (to prevent infringement of a patent), as well as submitting legal actions before the courts with or without interim measures or preliminary measures.

For copyright infringement, the injured party can, among other measures, request an administrative decision be handed down by the Spanish Copyright Commission, as well as file an arbitral procedure before international public bodies such as the WIPO (eg, in the case of domain name disputes). Likewise, they may also be entitled to file preventive letters (see Ruling No. 84/2020 handed down by Barcelona Mercantile Court No. 8, dated 25 February 2020) and they are entitled to file legal actions before the courts with or without interim measures or preliminary measures.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

No.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

The entry into force of Law No. 28/2022 to promote the start-up ecosystem has brought the following important tax incentives:

- a reduced corporate income tax rate of 15 per cent for the first fiscal year of positive taxable base and the following three fiscal years; and
- the stock options exemption for Spanish tax resident employees of the start-up has been improved from €12,000 to €50,000.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

Yes. Law No. 13/2022 establishes new obligations to provide information on clients to the tax administration in accordance with Directive 2011/16/EU (Directive on Administrative Co-Operation 8). This change may have a considerable impact in relation to the administrative costs faced by fintech companies, especially in services linked to cryptoassets.

Further, in the last budget bill (Law No. 31/2022) a reduced corporate income tax rate of 23 per cent has been implemented for those groups of companies whose net turnover in the immediately preceding tax period is less than €1 million as a whole.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

EEA nationals do not require a work or residence permit.

Non-EEA nationals must obtain work and residence permits to live and work in Spain. A range of licences can be issued by employers, each licence has its own specific requirements.

As a general rule, for the technology and financial sectors, the quickest and easiest way to recruit skilled staff from abroad is through the highly qualified foreign professionals (HQP) permit. This type of permit is for professionals who are graduates or postgraduates of universities and prestigious business schools who will be employed in Spain and whose fixed annual salary will be set at least at €50,000. The HQP permit has a streamlined process: according to the law, an application for a residence permit must be resolved by the Spanish authorities within a maximum of 20 working days from when it was duly registered, attaching all necessary documents. Once the permit has been granted, the candidate will need to request a visa at the Spanish consulate of the candidate's country of residence. Should the candidate be a legal resident in Spain at the time the work permit is submitted, the process would be even quicker as the visa step would not be needed.

UPDATE AND TRENDS

Current developments

41 Are there any other current developments or emerging trends to note?

There are no relevant developments to note.

Read this article on Lexology

* *The authors wish to thank Alfredo de Lorenzo and Álvaro Muñoz of Simmons & Simmons LLP for their assistance in the preparation of this chapter.*

Carmen Torres	carmen.torres@simmons-simmons.com
Ignacio González	ignacio.gonzalez@simmons-simmons.com
Juan Sosa	juan.sosa@simmons-simmons.com
María Tomillo	maria.tomillo@simmons-simmons.com
Raquel Ballesteros	raquel.ballesteros@simmons-simmons.com

Calle Miguel Angel 11, 5th floor, Madrid 28010, Spain
Tel: +34 91 426 2640
www.simmons-simmons.com

Read more from this firm on Lexology

Read this article on Lexology

Sweden

Emma Stuart-Beck, Nicklas Thorgerzon, Caroline Krassén and Anton Sjökvist

Vinge

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 531

General innovation climate 531
Government and regulatory support 532

FINANCIAL REGULATION 532

Regulatory bodies 532
Regulated activities 533
Consumer lending 534
Secondary market loan trading 535
Collective investment schemes 535
Alternative investment funds 536
Peer-to-peer and marketplace lending 536
Crowdfunding 536
Invoice trading 537
Payment services 537
Open banking 537
Robo-advice 537
Insurance products 538
Credit references 538

CROSS-BORDER REGULATION 538

Passporting 538
Requirement for a local presence 538

SALES AND MARKETING 539

Restrictions 539

CRYPTOASSETS AND TOKENS 540

Distributed ledger technology 540
Cryptoassets 540
Token issuance 541

ARTIFICIAL INTELLIGENCE 541

Artificial intelligence 541

CHANGE OF CONTROL 542

Notification and consent 542

Read this article on Lexology

FINANCIAL CRIME 542
Anti-bribery and anti-money laundering procedures 542
Guidance 543

DATA PROTECTION AND CYBERSECURITY 543
Data protection 543
Cybersecurity 544

OUTSOURCING AND CLOUD COMPUTING 544
Outsourcing 544
Cloud computing 545

INTELLECTUAL PROPERTY RIGHTS 545
IP protection for software 545
IP developed by employees and contractors 546
Joint ownership 547
Trade secrets 547
Branding 548
Remedies for infringement of IP 548

COMPETITION 548
Sector-specific issues 548

TAX 549
Incentives 549
Increased tax burden 549

IMMIGRATION 549
Sector-specific schemes 549

UPDATE AND TRENDS 550
Current developments 550

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

During its long history of fintech innovation, Sweden has produced companies such as Klarna, iZettle, Trustly, Tink, BehavioSec and Safello, to name a few. Innovation is diverse, and fintech products span areas such as banking services, payment and payment-settlement services, lending, biometrics and cryptocurrency. The private equity industry has a great appetite for Swedish fintech companies and the Swedish fintech industry is still growing rapidly. Multiple fintech companies have emerged within, inter alia, consumer lending and the Swedish housing credit market. The Swedish Financial Supervisory Authority (SFSA) has recently increased its focus on consumer lending and credit assessment.

In the wake of the economic uncertainties brought on by global events such as the war in Ukraine, the European energy crises and inflation, investors have become more cautious. This heightened risk aversion can be particularly challenging for fintech start-ups, which

Read this article on Lexology

often rely on their ability to attract large upfront investments to develop technology and establish a market presence.

Despite the potential regulatory and market challenges, the outlook for the Swedish fintech industry remains positive. With a strong track record of innovation and a supportive ecosystem of investors, entrepreneurs, and government agencies, Sweden is well-positioned to continue driving fintech innovation in Europe and beyond.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

The Swedish government has expressed interest in supporting and promoting the development of the Swedish fintech sector. During the second half of 2022, the Swedish Authority for Privacy Protection conducted their first pilot with a regulatory sandbox where they provided in-depth guidance to a specific innovation initiative on how the data protection legislation should be interpreted and applied. The work resulted in a public report where reasoning and assessments are summarised to enable learning for a broader audience. The sandbox was set up on the initiative of a report authored by a recently established Swedish government committee with the mission to help the government identify policy challenges, contribute to reducing uncertainty surrounding existing regulations, and accelerate policy development linked to the fourth industrial revolution technologies. While no similar sandbox has been implemented for financial regulations in general it does indicate a substantial and growing understanding at the regulator for the Swedish fintech industry. The SFSA has moreover introduced the SFSA Innovation Centre, which serves to act as a point of contact for fintech companies and to facilitate a dialogue with the SFSA. Further, the Innovation Centre is intended to provide guidance on applicable regulations for new financial services products and fintech start-ups.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

The Swedish Financial Supervisory Authority (SFSA) generally acts as the competent regulator responsible for the ongoing supervision of fintech products and services and for the issuance of supplementary regulations and formal guidance. The SFSA is responsible for ensuring that the business of (regulated) fintech companies is carried out in accordance with applicable laws and regulations, and the SFSA publicly announces when it is investigating a particular company for possible infringements.

All marketing activities that have the purpose of furthering the sale of any product in Sweden, including fintech products of various nature, are subject to the Marketing Practices Act (2008:486) (MPA), which requires, for example, that marketing is carried out in accordance with generally accepted marketing practices. The Swedish Consumer Agency, which

includes the Consumer Ombudsman, is the primary authority responsible for ensuring that marketing material is compliant with the MPA.

The Swedish Authority for Privacy Protection (SAPP) is the supervisory authority responsible for monitoring compliance with EU Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR) and supplementing regulations related thereto. The SAPP issues guidelines and regulations for the usage and processing of personal data and has become increasingly important for fintech companies as fintech services are often data-heavy. The SAPP's mandate includes all GDPR-related issues in Sweden. The SAPP may inspect companies and can issue fines under the GDPR.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

The following activities could trigger a licensing requirement:

- consumer lending and mediation;
- mortgage lending, mediation or advising;
- lending, factoring and invoice discounting in combination with accepting repayable funds from the public;
- deposit-taking;
- management of alternative investment funds (AIFs) or undertakings for collective investment in transferable securities (UCITS);
- insurance mediation;
- issuance of electronic money;
- provision of crowdfunding services;
- provision of payment services; and
- activities under EU Regulation (EU) No. 575/2013 (Capital Requirements Regulation).

Further, a licence is required for offering the services and products covered by Directive 2014/65/EU (Markets in Financial Instruments Directive II) (MiFID II), such as the reception and transmission of orders in relation to one or more financial instruments, the execution of orders on behalf of clients, dealing on own account, portfolio management, advising on investments in financial instruments, underwriting of financial instruments or placing of financial instruments on a firm commitment basis, and placing of financial instruments without a firm commitment basis.

The following activities could trigger a registration requirement:

- currency exchange;
- management or trading in virtual currencies;
- lending and mediation of credits to non-consumers as well as leasing and provision of guarantees and similar commitments (if not combined with accepting repayable funds from the public);
- issuing of means of payments;
- participating in securities issues;
- providing economic advice;
- safe custody services;

Read this article on Lexology

- operating a cryptocurrency trading platform; and
- foreign exchange trading.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Yes, consumer lending is regulated through, inter alia, the Consumer Credit Act (2010:1846), which includes relevant provisions relating to, among other things, sound lending practices, marketing of consumer loans, credit assessments, information prior to the conclusion of and in relation to the documentation of loan agreements, interest, fees and repayment of loans.

To offer or provide consumer loans, the relevant company is required to be authorised by the SFSA under the Consumer Credit (Certain Operations) Act (2014:275) (CCCOA) (should the company solely provide or act as an intermediary in relation to consumer loans), the Swedish Banking and Financing Business Act (2004:297) (SBFBA) (should the company instead, given the operations carried out, be considered a credit institution (as defined in the EU Capital Requirements Regulation or the Housing Credit Operations Act (2016:1024) (HCOA) (should the company solely provide, act as an intermediary in relation to or provide advice regarding consumer loans in the form of mortgages).

Sweden has rules regarding high-cost credits, which are defined as credits granted to consumers that have an interest rate of 30 percentage points above the reference rate according to the Interest Act (1975:635), as determined by the Swedish Central Bank, and that do not primarily relate to a credit purchase or residential immovable property.

The high-cost credits include certain caps where:

1 the maximum amount of interest, as well as any default interest, that may be charged under a credit agreement may not exceed 40 percentage points above the aforementioned reference rate; and
2 the maximum amount of fees under a credit agreement may not exceed the credit amount.

For the purposes of (2), fees are defined as costs for the credit (comprising the aggregate amount of interest rate, credit fees and other costs that the consumer is obliged to pay under the loan, inclusive of necessary costs for valuation but excluding notarisation fees), default interest and costs pursuant to the Compensation for Collection Costs Act (1981:739), comprising costs that the creditor has incurred for measures taken for the purposes of obtaining payment including, for example, payment reminders and collection demands.

The marketing of consumer credits is also subject to certain requirements regarding moderation and restraint. These rules include an explicit requirement for all such marketing to be moderate. This requirement is applicable to all types of consumer credits and, thus, not solely to high-cost credits (as defined above).

The authorities have paid more attention to the moderation requirement recently, and it is clear that a comprehensive assessment of all relevant circumstances will be made. In particular, the authorities and courts will assess:

- whether the credit is presented in a way that misleads the consumer about the financial consequences of the credit or brings the consumer to make an unfounded decision to enter into a credit agreement;
- whether the credit is presented as a carefree solution to the consumer's financial problems; and
- whether the credit is neutral in a way that enables the consumer to decide whether the credit is favourable or not.

Pursuant to the Swedish government preparatory works, it is stipulated that the marketing should be as neutral and factual as possible and may not be intrusive (by way of, eg, targeting certain types of possible consumers via digital means). The marketing should also be balanced in the sense that certain terms of the credit should not be disproportionately highlighted, thereby reducing the consumer's ability to make a well-founded decision.

In 2020, the SFSA introduced new consumer credit regulations that forbid payment service providers from presenting credit purchase as the first payment option, or to have it set as the default payment option for online purchases where an option to pay the goods or service directly is also available.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

There are no particular restrictions on trading loans in the secondary market in Sweden. However, on 18 February 2021, the SFSA stated that lenders that fund their lending by issuing bonds must now apply for a financing business licence under the SBFBA unless the bonds are subject to a transfer restriction preventing them from being acquired by the public.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Collective investment undertakings are regulated through the UCITS Act (2004:46), stipulating that the management of a Swedish UCITS, the sale and redemption of units in the fund and administrative measures relating thereto may only be conducted following authorisation from the SFSA (with foreign European Economic Area management companies authorised in their respective home state being able to rely on passporting regulations to carry out operations in Sweden).

Fintech companies would generally not fall within the scope of the above-mentioned regulatory regime.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Yes, alternative investment fund managers (AIFMs) are regulated through the Alternative Investment Fund Managers Act (2013:561) (AIFMA), implementing Directive 2011/61/EU (Alternative Investment Fund Managers Directive) (AIFMD). Small AIFMs (namely, AIFMs managing AIFs below the thresholds specified in article 3(2) of the AIFMD) may be exempted from the licensing requirements but must register with the SFSA and may not passport the registration into any other EU member state.

Similar to the case in relation to UCITS, fintech companies would generally not fall within the scope of the AIFMA.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Companies facilitating peer-to-peer or marketplace lending, comprising loan intermediation or brokering, are regulated by and require authorisation pursuant to the CCCOA (if the borrowers are consumers) or the HCOA (if the borrowers are consumers and the loans relate to purchases of residential immovable property). Both the CCCOA and the HCOA contain regulations on, for example, anti-money laundering measures (AML), sound practices for loan intermediation operations, and ownership and management assessments.

Business operators providing those services to borrowers that are not consumers are required to register their operations with the SFSA (by way of notification to the SFSA) in accordance with the Certain Financial Operations (Reporting Duty) Act (1996:1006) (CFORDA) and comply with provisions relating to, for example, AML, as well as undergo ownership and management assessments. Should the relevant company also be responsible for the transactions of funds between lenders and borrowers (including keeping funds on a client account, or similar), the operations would instead fall under and require authorisation pursuant to the Payment Services Act (2010:751) (PSA), which imposes additional requirements relating to, for example, own funds and information and technical processes relating to the execution of payment transactions.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

Regulation (EU) 2020/1503 on Crowdfunding Service Providers (the Crowdfunding Regulation) establishes a harmonised framework for crowdfunding service providers in the European Union. Particular for the Swedish market as regards the Crowdfunding Regulation is that, due to the prohibition in the Companies Act (2005:551) for Swedish private companies or shareholders from attempting to sell shares or subscription rights in the company or debentures or warrants issued by the company to the public, shares in such companies would not be admitted instruments for crowdfunding purposes as referred to in the Crowdfunding Regulation.

Read this article on Lexology

Invoice trading

11 Describe any specific regulation of invoice trading in your jurisdiction.

In accordance with the CFORDA, a company participating in financing, for example, by acquiring claims (invoice trading), is required to register its operations with the SFSA (by way of notification to the SFSA), and it is further obliged to comply with provisions relating to, for example, AML, and to undergo ownership and management assessments.

A public inquiry relating to the Swedish implementation of Directive (EU) 2021/2167 on credit servicers and credit purchasers was published in January 2023, suggesting inter alia regulations of the secondary market of non-performing loans.

Payment services

12 Are payment services regulated in your jurisdiction?

Yes. Payment services are regulated under Directive (EU) 2015/2366 (Second Payment Services Directive) (PSD2), which has been implemented into Swedish law through the PSA. The PSA regulates services enabling cash to be place on or withdrawn from a payment account as well as all the operations required for operating a payment account, execution of payment transactions, issuing of payment instruments, acquiring of payment transactions, money remittance, payment initiation services and account information services.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

As required per PSD2, the PSA requires account servicing payment service providers to allow account information service provider access to a payment accounts. Sweden has not gone beyond PSD2 as regards the rights to data.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

There is no specific regulation of automated investment advice in Sweden. The SFSA defines automated investment advice as personal advice regarding financial instruments that is provided without, or with limited, human interaction. In Sweden, automated investment advice (eg, robo-advice) constitutes regulated investment advice under the Securities Markets Act (2007:528), implementing MiFID II, and is consequently subject to all the substantive provisions of the Swedish MiFID II implementation, including the SFSA's regulations regarding investment services and activities (2017:2).

Read this article on Lexology

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Yes, if the selling and marketing is classified as 'insurance distribution'. Insurance distribution is regulated under the Insurance Distribution Act (2018:1219) (IDA) implementing Directive (EU) 2016/97 (Insurance Distribution) (IDD). The IDD is a minimum harmonisation directive, enabling member states to impose stricter regulation. The IDA includes the same definition of 'insurance distribution' and the same exemptions from regulation as the IDD. Typically, marketing that is not covered by the scope of the IDA is characterised by the fact that it is not possible for a potential customer to, directly or indirectly, take out an insurance in connection with the marketing measure. If an insurance can be taken out in connection with the marketing measure, it will constitute insurance distribution unless the exemptions of ancillary insurance distribution apply. Sweden has imposed stricter regulations regarding third-party remunerations, conditions for providing advice on a fair and personal analysis, certain marketing prohibitions and information to a customer on remuneration. The stricter regulatory framework introduced by the IDD regarding insurance-based investment products also applies to the distribution of pension insurance that is exposed to market volatility.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Yes. Credit references and credit information services are regulated under the Credit Information Act (1973:1173) and the Credit Information Regulation (1981:955). A licence from the SAPP is required when carrying out credit-rating operations in Sweden.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

Yes. An undertaking that has been authorised in its home EU member state may, as a general rule, passport such authorisation into Sweden, where the Swedish legislation is based on EU law.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

An undertaking that has been authorised in its home EU member state may, as a general rule, passport such authorisation into Sweden, where the Swedish legislation is based on EU law. However, in relation to activities that fall under the Consumer Credit (Certain Operations) Act, a Swedish licence is required (namely, passporting is not available).

Read this article on Lexology

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Marketing of financial services falls under the Marketing Act (2008:486) (MPA), which applies to all marketing activities that have the purpose of furthering the sale of any product or service in Sweden, including, for example, the distribution of brochures and other marketing materials and electronic marketing activities (if primarily directed to Swedish entities or individuals). The MPA provides that all marketing must be consistent with good marketing practice and be fair and reasonable towards the person to whom or to which it is directed.

Good marketing practice is defined in the MPA as generally accepted business practices or other established norms aimed at protecting consumers and traders in the marketing of products. Thus, all marketing must be designed and presented in such a way as to make it apparent that it constitutes marketing and the party responsible for the marketing shall be clearly indicated. Statements or other descriptions that are or may be misleading may not be used. Marketing that contravenes good marketing practice is regarded as unfair if it appreciably affects or probably affects the recipient's ability to make a well-founded transaction decision.

In relation to financial services, and to comply with 'good marketing practice' for the purposes of the MPA, among other things:

- placements of capital or returns should not be described in terms such as 'safe', 'guaranteed' or similar value judgements if it cannot be verified that it is guaranteed that an investor's capital will be repaid or that a given return will be earned;
- the return earned during a particularly successful period on an investment product should not be highlighted in a way that gives a distorted overall impression of the performance of the investment product;
- words such as 'secure' and similar value judgements should not be used for marketing purposes if they are not placed in a relevant context;
- unconditional words expressing value, such as 'best', 'biggest' and 'leading', should not be used if the claim is not capable of verification; and
- if an investment product involves risk, it should always be made clear when marketing the product that an investment in the product involves risk.

In addition, the marketing of funds is further specifically regulated through the Swedish Investment Fund Association's guidelines, which – albeit not being hard law – are considered as codifying good marketing practices in Sweden in respect of the marketing of undertakings for collective investment in transferable securities.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

There are no rules or guidelines specifically addressing the use of distributed ledger technology, but general rules and regulations, such as anti-money laundering (AML) regulations and consumer protection, where applicable, must be complied with. The Swedish Financial Supervisory Authority (SFSA) has, in a report from March 2016, identified distributed ledger or blockchain technology as an area of interest for the supervisor and where it is expected that rules and regulations need to be adopted in the future. If the distributed ledger technology or blockchains include personal data, general requirements under EU Regulation (EU) 2016/679 (General Data Protection Regulation) and Swedish data protection laws will be applicable.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

There is currently no generally accepted definition of cryptoassets in Swedish regulations, nor is there a generally applicable regulatory framework available. Further, the Swedish legislator is unlikely to introduce a more comprehensive national framework given the thorough regulations proposed in the European Commission's Regulation of Markets in Crypto-assets.

The Certain Financial Operations (Reporting Duty) Act (1996:1006) (CFORDA) does, however, contain some provisions explicitly covering certain activities with virtual currencies that would generally encompass cryptoassets. Pursuant to the preparatory works of the CFORDA, virtual currencies shall generally be understood as they are defined in Directive (EU) 2018/843 (Fifth Anti-Money Laundering Directive), namely, as a digital representation of value that is not issued or guaranteed by a central bank or a public authority, not necessarily attached to a legally established currency and not possessing a legal status of currency or money, but that is accepted by natural or legal persons as a means of exchange and that can be transferred, stored and traded electronically. The SFSA has stated on its website that this would include bitcoin and ether.

The activities covered by the CFORDA are the management of, or the trading in, virtual currencies. This would, for example, be the exchange of virtual currencies for fiat currencies or other virtual currencies, or the provision of custodian wallets for virtual currencies. The significance is that these activities would be subject to a registration requirement, mainly so that they would be covered by the Swedish AML regime. However, an assessment would also need to be made to determine whether the activities and cryptoassets involved would qualify for any of the other regulatory frameworks available. As such, depending on the activities and the nature of the cryptoassets involved, the Securities Markets Act (SMA), the Electronic Money Act (2011:755) (EMA) or the Payment Services Act (2010:751) (PSA) could apply.

Read this article on Lexology

The SFSA has shown an increased interest in the subject of cryptoassets lately and has warned consumers from acquiring such assets twice during 2021, as well as produced a report about financial instruments with cryptoassets as underlying assets (tracker certificates), due to the risks involved for consumers in investing in such assets. Therein, the SFSA has highlighted that there is a current lack of protection for consumers in transactions involving cryptoassets as most of those are unregulated. In addition, the SFSA arranged for a meeting with market participants in May 2021 to have a dialogue regarding the development of the market of cryptoassets and what possibilities and challenges are associated therewith. The SFSA's interest in the subject is only likely to increase going forward as trading in cryptoassets increases.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

There is no specific regulation of digital currency exchanges or brokerages but activities involving the exchange of virtual currencies for other virtual currencies or fiat currencies would normally be subject to the CFORDA. Where the provider of the digital currency exchange performs payment services as part of the exchange, the PSA would also be applicable. Depending on the activities provided and the nature of the digital currency involved, the activities could also be encompassed by the SMA or the EMA.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

There is no specific regulation of automated investment advice in Sweden. The Swedish Financial Supervisory Authority (SFSA) defines automated investment advice as personal advice regarding financial instruments that is provided without, or with limited, human interaction. In Sweden, automated investment advice (eg, robo-advice) constitutes regulated investment advice under the Securities Markets Act and is consequently subject to all the substantive provisions of the Swedish implementation of Directive 2014/65/EU (Markets in Financial Instruments Directive II), including the SFSA's regulations regarding investment services and activities (2017:2). If the use of artificial intelligence would include decisions based solely on automated processing of personal data, including profiling, this would be subject to the requirements in article 22 of EU Regulation (EU) 2016/679 (General Data Protection Regulation).

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Consent from the Swedish Financial Supervisory Authority (SFSA) is required where a legal or natural person intends to directly or indirectly acquire a qualified holding in a regulated business.

The holding is considered qualified when the acquirer directly or indirectly receives 10 per cent or more of the votes or shares, or otherwise is enabled to exercise significant influence over the management of the regulated business. Additional consent is required if the ownership amounts to or exceeds 20, 30 or 50 per cent of the votes or shares.

The consent requirement, generally referred to as an 'ownership assessment', means that the SFSA will examine all qualified owners in the envisaged ownership chain. The process is rather extensive, and the exercise involves collating and producing a substantial amount of information (including documentation that supports the financing of the transaction). Each person included in the management body (comprising board members, the chief executive officer and the deputies thereof) of an entity subject to assessment must complete and sign an application, including responding to questions regarding, for example, previous criminal proceedings.

SFSA consent must be obtained prior to the transaction. The SFSA has an expected processing period for the applications of 60 business days, with a possible extension of 20 business days if the SFSA requests additional information during the assessment process.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Companies licensed by or registered with the Swedish Financial Supervisory Authority (SFSA) and a significant number of companies and other professionals outside the financial sector are obligated to prevent money laundering and financing of terrorism by complying with the Money Laundering and Terrorist Financing Prevention Act (2017:630) and subsequent regulations. Pursuant to the anti-money laundering (AML) regulations, companies are required to adopt internal AML procedures. Companies launching initial coin offerings would be subject to these requirements to the extent their operations would be covered by any of the relevant rules under, for example, the Certain Financial Operations (Reporting Duty) Act and the Securities Markets Act.

The SFSA is tasked with ensuring that the financial companies adhere to the AML regulations. The County Administrative Board supervises companies and professionals outside the financial sector.

Bribery is criminalised under the Penal Code (1962:700), which is applicable to all types of Swedish companies. Most financial companies are required to adopt ethical guidelines setting out, inter alia, the company's procedures to combat bribery.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

Yes. The SFSA has adopted regulations and guidelines in respect of AML, setting out the detailed provisions applicable for relevant companies.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

EU Regulation (EU) 2016/679 (General Data Protection Regulation) (GDPR) and the Swedish Act on Supplementary Provisions to the GDPR (2018:218) generally apply to the processing of personal data by data controllers established in Sweden. The main requirements relating to the processing of personal data include the following:

- personal data may only be processed (namely, collected, used and stored) if there are legal grounds (namely, consent) for the processing. However, there are several exemptions from the requirement of consent (eg, where the processing is necessary to fulfil a contract or a legal obligation or is necessary to pursue a legitimate interest of the data controller, unless this interest is overridden by the interest of the registered person to be protected against undue infringement of privacy);
- certain fundamental requirements must be met (eg, personal data must be adequate, relevant and non-excessive in relation to the purpose of the processing and must not be kept longer than necessary);
- data subjects must, as a general rule, be informed of the processing of their personal data, and data subjects have certain rights (eg, right of access, rectification, erasure and data portability);
- processing of sensitive personal data and criminal offence data may only be performed in limited circumstances. In general, consent from the person concerned is required for sensitive data. As a general rule, it is prohibited to process criminal offence data (there are a few exemptions, for example, regarding whistle-blowing systems, where it is permitted to process criminal offence data under certain conditions);
- there are specific requirements that must be met in the case of the export of personal data to countries outside the European Union or the European Economic Area (eg, consent or model clause agreements may justify such export);

Read this article on Lexology

- a data controller must take appropriate technical and organisational measures to protect personal data. Data processing agreements must be entered into with data processors;
- the GDPR also includes requirements regarding, inter alia, the appointment of data protection officers, personal data breaches, data protection by design and by default, records of processing activities, data protection impact assessments, consultation and cooperation with the data national protection authority; and
- the GDPR applies to pseudonymised data but not to fully anonymised data (namely, where it is not possible to directly or indirectly identify an individual by any means).

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

Under the GDPR, controllers must have 'appropriate technical and organisational measures' in place to ensure a level of security appropriate to the risk. There is, therefore, no prescribed level of security, but analysis must be carried out to ascertain what level of security is appropriate to the type of processing of personal data being carried out.

Directive (EU) 2016/1148 on security of network and information systems (NIS Directive) has been implemented into Swedish law (2018:1174) and supplemented by a regulation (2018:1175). These acts impose cybersecurity requirements for digital services providers and operators of essential services. Companies in the finance industry that are deemed as operators of essential services within the banking or financial market infrastructure are covered by these acts and are, therefore, obliged, among other things, to:

- notify the Swedish Financial Supervisory Authority immediately;
- demonstrate a systematic and risk-based approach to matters regarding information security; and
- report incidents to the Swedish Civil Contingencies Agency.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

There are multiple legal and regulatory requirements in respect of outsourcing by financial services companies, including, inter alia:

- the Swedish Banking and Financing Business Act (2004:297);
- the Consumer Credit (Certain Operations) Act (2014:275);
- the Swedish Securities Markets Act (2007:528);
- the Electronic Money Act (2011:755);
- the Payment Services Act (2010:751);
- the Swedish Financial Supervisory Authority (SFSA) regulations;

- detailed provisions set out in EU Delegated Regulation (EU) 2017/565 and the European Banking Authority (EBA) Guidelines on Outsourcing Arrangements (EBA/GL/2019/02); and
- questions and answers provided by the SFSA on the application of the EBA guidelines.

The provisions are subject to some variation, but in general impose that financial services companies are required to exercise the requisite skill, care and diligence when entering into, managing and terminating outsourcing arrangements. Further, the rights and obligations of the financial services company and the services provider must be clearly documented in an outsourcing agreement. If the financial services company intends to outsource a significant part of the licensed operations, or activities that have a natural connection with financial operations or their support functions, the financial services company is required to notify the SFSA thereof in advance and also provide the SFSA with a copy of the relevant outsourcing agreement.

The SFSA requires outsourcing agreements to be in writing and to regulate clearly the rights and obligations of the financial services company and the third-party service provider. The SFSA further expects the financial services company to be able to assess and monitor how well the third-party service provider is carrying out its duties and to terminate the agreement should the third-party service provider lack the skills, capacity and authorisations required by law to reliably and professionally perform the outsourced duties and manage risks related to these duties.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

The EBA Guidelines, applicable for institutions, electronic money institutions and payment institutions, offer guidance in respect of outsourcing to cloud service providers and have integrated and replaced the previously issued EBA Recommendations on Outsourcing to Cloud Service Providers (EBA/REC/2017/03). On 18 December 2020, the European Securities and Markets Authority issued its Final Guidelines on Outsourcing to Cloud Service Providers for, inter alia, investment firms and credit institutions that carry out investment services and activities.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Computer programs are protected as copyrighted works in accordance with the Copyright Act (1960:729) (CA). Copyright protection arises automatically, and there is, thus, no registration procedure for obtaining copyright protection.

Software-implemented inventions and business methods can be registered and protected as patents if they meet all the necessary requirements. Computer program code or mere

business methods, however, cannot be patented in Sweden, but a technical invention that includes a business method, or which is implemented or can be implemented by a computer program, can be patentable.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

In general, intellectual property developed during the course of employment vests with the employee unless explicitly transferred to the employer. However, the employer has a more or less extensive right to acquire or utilise the intellectual property depending on the category of intellectual property and the category of the invention as well as the provisions in the applicable employment or collective bargaining agreements. There are also specific statutory provisions concerning certain intellectual property. Below is a summary of the general principles regarding an employer's rights to inventions developed by its employees.

According to the CA, copyright in a computer program created in the course of employment is automatically transferred to the employer unless otherwise agreed in, for example, the employment agreement. However, the scope of the concept of 'computer program' is not clear under Swedish law. Therefore, it is recommended that employers include an appropriate clause in the employment agreement that explicitly transfers all rights to the employer.

It should be noted that there are some new provisions in the CA regarding employees right to fair compensation after transfer of copyright works to the employer, employees right to subsequent information about the transferred copyright works and employees right to terminate an agreement through which a copyright work has been transferred to the employer. However, these new provisions do not apply to copyright in computer programs.

An employer has certain rights to patentable inventions developed by its employees. Those inventions are divided into three categories, and the employer's rights differ between the categories:

- inventions developed by employees that are employed to conduct research and development work, and which are developed within the scope of employment, may be acquired or utilised by the employer;
- inventions developed within the employer's line of business but developed by an employee that is not employed to conduct research and development work may be utilised by the employer, and the employer has priority over others in acquiring ownership of the invention; and
- inventions developed within the employer's line of business but developed without any connection to the employment may be acquired by the employer, with priority over others, if agreed upon with the employee.

Collective bargaining agreements (if applicable) may also contain provisions on employers' rights to intellectual property developed by employees similar to the three categories described above.

Read this article on Lexology

In relation to contractors and consultants, the main rule is that all rights in results vest in the originator. This means that a company must explicitly acquire the rights to those results through agreements with the originator. The inclusion of appropriate intellectual property clauses in the agreement with contractors and consultants are, thus, essential.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

The Swedish legislation does not fully regulate the matter of joint ownership of intellectual property. Only the CA regulates the matter explicitly, whereby the main rule is that co-authors have a joint right to the copyright-protected work. The same should reasonably also apply to the other categories of intellectual property.

Unless agreed otherwise between the co-owners, the Act on Joint Ownership (1904:48) (AJO) is applicable. The AJO states that consent from all co-owners is necessary for all decisions concerning the management of the jointly owned property. All co-owners are, however, entitled to sell their share in the jointly owned intellectual property without consent from the other owners.

In light of this, co-owners of intellectual property are restricted from utilising, licensing, charging or assigning the intellectual property in whole without the other co-owner's consent. The co-owners must, thus, settle the joint ownership and agree on how to use and manage the intellectual property to avoid uncertainty.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Protection for trade secrets is granted through the Trade Secrets Act (2018:558) (TSA). For the purposes of the TSA, trade secrets are defined as information concerning the business or operational circumstances in a trader's business, which is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question, which the trader has taken reasonable measures to keep confidential and the disclosure of which is likely to cause damage to the trader from a competition perspective. Trade secrets cannot be registered for protection, and the only statutory protection for such information is granted under the TSA.

Court proceedings, as well as all evidence and other information submitted to the court, are generally public in Sweden. However, for information concerning the business or operational circumstances, the parties may request secrecy when submitting information or during the proceedings as well as afterwards. However, a Swedish court is not required to adhere to such request, and there is no way of knowing whether the court will grant a request of secrecy in advance.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

The general provisions for the protection of trademarks and trade symbols are provided in the Trademarks Act (2010:1877). A trade symbol can be registered for protection in Sweden if it is distinctive (namely, capable of distinguishing goods or services of one business activity from those of another). A trademark registered for protection in the European Union also grants protection in Sweden. Exclusive rights to a trade symbol may also be obtained, without registration, if the symbol is considered established on the market. A trade symbol is deemed established on the market if it is known by a significant part of the relevant public as an indication of the goods or services that are being offered under it.

New businesses can either perform searches themselves in relevant public databases for trademarks identical or similar to the trademarks they intend to use (eg, in the Swedish Patent and Registration Office's database, which covers both Swedish and EU trademarks) or engage a trademark attorney to assist with such preliminary investigations.

General branding can be protected by the Marketing Act (2008:486). The Act protects against unfair competition and can, thus, inter alia, protect a business against other businesses taking unfair advantage of the reputation associated with the first business, including its trademark, business name or other distinctive marks.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

There are numerous remedies available when suing an alleged infringer in court. For example, preliminary injunctions and prohibitions under penalty of a fine as well as damages for infringement, loss of profit and impaired goodwill are available in all Swedish intellectual property laws. Infringements committed intentionally or through gross negligence can also result in fines or imprisonment.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

There are no specific competition rules for fintech companies. The general Swedish competition rules, which are based on EU competition law, apply. The rapid growth of the Swedish fintech industry in recent years has given rise to many new payment solutions and increased competition between the old and the new. Although we have seen issues relating, inter alia, to the interoperability between the traditional banking systems and the new digital

solutions, case law regarding the application of the competition rules in the fintech industry is still limited.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

There are no special Swedish tax incentives for fintech companies or investors to encourage innovation and investment in the fintech sector in Sweden.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

No.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

There are no specific immigration schemes available for fintech businesses to recruit skilled staff, nor are there any special regimes specific to the technology or financial sectors. Whether a work permit is required for the specific role is subject to a case-by-case assessment. The main rule under Swedish law is that for a citizen of a non-EU country to be able to work and reside in Sweden, a work permit and a residence permit are required. EU citizens are, however, entitled to work in Sweden without any kind of permit. Swiss citizens are entitled to work in Sweden without a work permit, but are still required to apply for a residence permit (if the stay is longer than three months).

Certain other categories of employees may also temporarily work in Sweden without a specific work permit, provided that certain requirements are fulfilled. For example, a work permit is not required for individuals employed by a multinational corporate group where the employees will undergo practical training, on-the-job training or other in-service training at a company in Sweden that is part of the group (a maximum aggregate period of three months over a period of 12 months). In the absence of any of the aforementioned exemptions, all non-EU citizens must obtain a work permit to be entitled to work in Sweden.

The application procedure is generally the same for all applicants regardless of occupation or industry. Applications are assessed by the Swedish Migration Agency (MA), and

the application processing time varies. It currently takes six to nine months for the MA to examine a complete first-time application registered through the regular queue. There are, however, particular certified firms (such as certain law firms) with access to the MA's fast-track system when applying for work permits on behalf of a client company and its employees. Certified firms are entitled to a significantly shorter turnaround time (10 days for complete first-time applications). In cases where the employer is not bound by a collective bargaining agreement and the concerned Swedish trade union does not oppose the absence thereof, the official fast-track turnaround time is 60 days.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

The Swedish National Bank has, further, owing to the marginalisation of cash usage in Sweden, initiated a pilot project to construct a technical platform for the e-krona, based on distributed ledger technology. A committee was appointed to investigate a general transition towards the digitalisation of currency in Sweden but has advised against adopting an e-krona. In addition, the Nordic P27 project, aiming to form the world's first integrated region for domestic and cross-border payments in multiple currencies through a common payments infrastructure, has been shut down.

Following recent developments in the global financial markets, it has proven more difficult for fintech firms and start-ups to raise capital. This may eventually lead to more consolidations and an increased focus on cost savings rather than expansion. Although the market developments in recent years have led to consolidations, mergers and several start-ups facing a more challenging environment racing capital. Sweden in general – and Stockholm in particular – are still vibrant for fintech companies, and the coming years may provide for further developments on the Swedish fintech scene.

VINGE

Emma Stuart-Beck emma.stuart-beck@vinge.se
Nicklas Thorgerzon nicklas.thorgerzon@vinge.se
Caroline Krassén caroline.krassen@vinge.se
Anton Sjökvist anton.sjokvist@vinge.se

Smålandsgatan 20, Stockholm 111 87, Sweden
Tel: +46 10 614 30 00
www.vinge.se

Read more from this firm on Lexology

Read this article on Lexology

Switzerland

Luca Dal Molin, Daniel Haeberli, Stefan Oesterhelt, Richard Stäuber, Manuel Baschung and Alexander Wherlock

Homburger

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 552

General innovation climate 552
Government and regulatory support 553

FINANCIAL REGULATION 554

Regulatory bodies 554
Regulated activities 554
Consumer lending 555
Secondary market loan trading 556
Collective investment schemes 556
Alternative investment funds 557
Peer-to-peer and marketplace lending 557
Crowdfunding 557
Invoice trading 558
Payment services 558
Open banking 559
Robo-advice 559
Insurance products 560
Credit references 560

CROSS-BORDER REGULATION 560

Passporting 560
Requirement for a local presence 560

SALES AND MARKETING 561

Restrictions 561

CRYPTOASSETS AND TOKENS 561

Distributed ledger technology 561
Cryptoassets 562
Token issuance 563

ARTIFICIAL INTELLIGENCE 564

Artificial intelligence 564

CHANGE OF CONTROL 565

Notification and consent 565

Read this article on Lexology

FINANCIAL CRIME 566
Anti-bribery and anti-money laundering procedures 566
Guidance 566

DATA PROTECTION AND CYBERSECURITY 567
Data protection 567
Cybersecurity 567

OUTSOURCING AND CLOUD COMPUTING 568
Outsourcing 568
Cloud computing 568

INTELLECTUAL PROPERTY RIGHTS 568
IP protection for software 568
IP developed by employees and contractors 569
Joint ownership 569
Trade secrets 569
Branding 570
Remedies for infringement of IP 570

COMPETITION 570
Sector-specific issues 570

TAX 571
Incentives 571
Increased tax burden 571

IMMIGRATION 571
Sector-specific schemes 571

UPDATE AND TRENDS 572
Current developments 572

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

In Switzerland, the government's general attitude towards fintech, and blockchain technology in particular, is very positive. Both the Swiss federal government and the Swiss Financial Market Supervisory Authority (FINMA) recognise the potential that fintech and blockchain technology offer to the Swiss financial services industry and various other areas of the economy. Switzerland sees an opportunity to take a global lead in this sector, evidenced by recently enacted legislation and various governmental initiatives in the fintech sphere. Switzerland is also increasingly becoming an international hub for research in the areas of fintech and technical innovation in general. Google, IBM, Disney, Thomson Reuters and the Federal Institute of Technology ETH have all established research centres in and around Zurich. Further, the University of Zurich has formed the UZH Innovation Hub, a platform for innovation and entrepreneurship, with a focus on digitisation in particular. Numerous Swiss financial service providers and major Swiss banks, such as Credit Suisse and UBS have

Read this article on Lexology

established innovation centres and have expanded their digital offerings in recent years. With SIX Swiss Exchange and BX Swiss, Switzerland also has two trading venues that are becoming increasingly attractive for the issuance of crypto-related exchange-traded products, with 21Shares and Hashdex – two major issuers of crypto-related structured products – generating a considerable trading volume in Switzerland. Finally, in late 2021, FINMA granted SIX Digital Exchange (SDX), a licence to operate a stock exchange and a central securities depository for digital assets in Switzerland. Under this licence, SDX offers a fully regulated trading, settlement and custody infrastructure based on distributed ledger technology for digital securities.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Swiss government bodies and regulators have implemented various initiatives aiming to enhance financial innovation in Switzerland. The most comprehensive project is Digital Switzerland, which coordinates various private initiatives and provides government support. Further, FINMA has established a designated fintech desk as a competence centre within FINMA for fintech-related applications and enquiries.

In 2018, FINMA issued specific guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) under which FINMA specified its practice regarding the regulatory treatment of ICOs (FINMA Guidelines). In a supplement to the FINMA Guidelines published in 2019, FINMA provided further guidance on the treatment of stablecoins under the financial market laws of Switzerland. Finally, in 2021, the Distributed Ledger Technology Law (the DLT Law) entered into effect in Switzerland. The DLT Law constitutes an 'umbrella legislation' that introduces a new concept of 'DLT securities' under the Swiss Code of Obligations allowing for the tokenisation of rights, claims and financial instruments. In addition, the DLT Law provides for the introduction of a new licensing category as a DLT trading venue under the Financial Market Infrastructure Act and certain clarifications relating to the treatment of cryptocurrencies in Swiss insolvency proceedings.

The Swiss National Bank (SNB) has done substantial research and carried out feasibility studies in relation to the potential use of digital central bank money. This new form of digital central bank money may allow the settlement of 'tokenised' assets between financial institutions. A first feasibility study as carried out under the project name Helvetia between the SNB and the SIX Group and successfully demonstrated the feasibility of settling tokenised assets with wholesale central bank digital currencies. In a second phase of Project Helvetia, SNB and SIX Group, together with Citi, Credit Suisse, Goldman Sachs, Hypothekarbank Lenzburg and UBS, explored and further analysed settlement of interbank, monetary policy and cross-border transactions on the test systems of SDX, the Swiss real-time gross settlement system – SIX Interbank Clearing – and core banking systems.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

Switzerland has not enacted a comprehensive framework governing the provision of fintech or crypto-related financial services. Such activities are subject to the general Swiss financial market laws and regulatory licensing requirements. The Swiss Financial Market Supervisory Authority (FINMA) is the competent prudential supervisory authority for banks, securities firms, asset managers and insurance companies. Further, various recent initial coin offerings (ICOs) were executed through foundations domiciled in Switzerland. Foundations incorporated under the laws of Switzerland are supervised by separate supervisory authorities at communal, cantonal and federal levels. Foundations established for the purpose of executing an ICO are typically supervised by the Federal Authority for Foundation Supervision.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Regardless if business activities performed by a fintech company qualify as a regulated activity in Switzerland, they will need to be assessed on a case-by-case basis. Fintech companies often fall into one of the following licensing categories.

Banking licence

Under the Federal Act on Banks and Savings Institutions (FBA), only licensed banks are permitted to accept deposits from the public on a professional basis. Pursuant to the FBA and the Federal Ordinance on Banks and Savings Institutions, the acceptance and storage of cryptoassets, as well as related custody services, qualify as regulated deposit-taking. Therefore, any fintech company that accepts deposits or provides custody services in relation to cryptoassets, on a professional basis, will – subject to certain exemptions – require a banking licence under the FBA. In addition to the regular banking licence, permitting the holder to engage in regulated banking activities, the FBA provides for a (simplified) fintech licence. The fintech licence permits the respective licence holder to accept deposits up to the threshold of 100 million Swiss francs or cryptoassets, provided that the deposits or cryptoassets are not invested and are not interest-bearing. If the maximum deposit threshold of 100 million Swiss francs is exceeded, the company must notify FINMA within 10 days and must apply for a regular bank licence within 90 days. With the fintech licence, companies not engaging in the classic banking business (interest rate differential business), for example, by using short-term deposits for long-term lending or investment activities, now have a viable regulatory alternative under which such companies can implement their business model.

Securities firm licence

Under the Federal Act on Financial Institutions (FinIA), only licensed securities firms are permitted to engage in regulated securities dealing. A fintech company will qualify as a securities firm, requiring a licence under FinIA, if it engages, on a commercial basis, in either:

Read this article on Lexology

- dealing in securities in its own name but on its clients' account;
- dealing in securities on a short-term basis on its own account and thereby either:
    - impacting the systemic stability of the Swiss financial market; or
    - being directly admitted to a trading venue within the meaning of the Financial Market Infrastructure Act (FMIA); or
- market-making activities.

In light of the outlined legal framework, fintech companies will typically require a licence as a securities firm, if their business model includes trading of digital assets, qualifying as 'securities' within the meaning of the FMIA, for the account of their clients. Under Swiss law, securities are financial instruments that are standardised and suitable for mass trading. Pursuant to FINMA's practice, to the extent that digital assets grant a claim against the relevant issuer, namely derivative financial instruments, such as futures, relating to cryptocurrencies, that are suitable for mass trading, such digital assets will qualify as securities within the meaning of Swiss law.

Licensing requirements under the Financial Market Infrastructure Act

Operating a platform that offers multilateral trading in securities within the meaning of the FMIA in Switzerland requires a licence as a trading venue (stock exchange or multilateral trading facility). A trading venue is an institution for multilateral trading in securities whose purpose is the simultaneous exchange of bids between several participants and the conclusion of contracts based on non-discretionary rules. Fintech companies operating a platform that offers trading in digital assets may require a licence as a trading venue, if the instruments traded on such platform qualify as 'securities' within the meaning of the FMIA (see also above). To the extent the financial instruments for which trading is offered do not qualify as securities, such trading systems may, depending on the relevant set-up, qualify as an organised trading system, which pursuant to the FMIA, may only be operated by Swiss-licensed banks and securities dealers. It should also be noted that trading venues domiciled outside Switzerland require a formal recognition by FINMA, if they admit Swiss-supervised entities to their trading facilities. Finally, in 2021, a new licence category, the distributed ledger technology (DLT) trading venue, was introduced under the FMIA. Licensed DLT trading venues are authorised to provide services in the areas of trading, clearing, settlement and custody of ledger-based securities to both regulated and unregulated financial market participants, including retail investors

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Generally, the granting of loans on a commercial basis is considered financial intermediation, which is subject to the Federal Anti-Money Laundering Act (AMLA). Thereunder, the financial intermediary is, namely, subject to the duty:

- to become a member of a self-regulatory organisation;
- to determine the identity of the contracting party and the beneficial owner of the transferred assets; and

- to clarify the financial background and purpose of the business relationship or transaction, if the financial intermediary becomes aware of indications that the funds in question were obtained through criminal activities or are intended to finance terrorism.

Further, the Federal Act on Consumer Credits (CCA) stipulates the general substantive rules governing consumer credits and sets out the supervisory licensing requirements for providers of consumer credits in Switzerland. Under the CCA, consumer credit providers (and arrangers of consumer credits) are subject to a number of obligations, namely the duty to determine the creditworthiness of the consumer, formal requirements applicable to the credit agreements, rules governing the calculation of interest payments and respective maximum interest thresholds. The CCA sets out sanctions in the case of a violation of such duties. The provision of consumer loans to consumers in Switzerland is subject to a licensing requirement. The licensing requirement is triggered by the provision or the solicitation of a consumer credit to a consumer domiciled in Switzerland. To obtain a licence under the CCA, the credit provider must:

- ensure an irreproachable conduct of business operations in Switzerland;
- have sufficient education and experience in the area of financial services; and
- have adequate liability insurance or provide respective securities.

Further, the credit provider must hold common equity tier 1 capital in the higher amount of:

- 8 per cent of the credit outstanding in Switzerland; or
- at least 250,000 Swiss francs.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

The trading of loans or participations therein on the secondary market is not subject to a licensing requirement in Switzerland.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

In Switzerland, the offering of units in a collective investment scheme is governed by the Federal Act on Collective Investment Schemes (CISA) and the FinIA, with licensing requirements applying both at the level of the fund, the fund management company and the asset manager for collective investment schemes. Pursuant to CISA, a financial instrument qualifies as a collective investment scheme for the purposes of Swiss law if it meets the following five criteria: (1) assets (2) that are raised from at least two independent investors (3) for the purpose of being collectively managed (4) for the account of such investors, (5) whereby the investors' investment needs are met on an equal basis.

Typically, the products offered by fintech companies, such as peer-to-peer lenders, marketplace lenders or crowdfunding platforms, do not qualify as collective investment schemes and will not be subject to CISA. In contrast, in cases where the business model of a fintech company involves the pooling of funds or risks in connection with an investment, such activities will likely be subject to CISA and the requirements set out thereunder.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

The Alternative Investment Fund Managers Directive is not applicable in Switzerland. However, pursuant to the FinIA, companies, managing funds and collective investment schemes, in their own name but for the account of its clients, require a licence as a fund management company. In addition, asset managers providing asset and risk management services to collective investment schemes require a licence as a manager of collective assets and are subject to prudential supervision by FINMA. To the extent that the managed collective investment schemes are limited to qualified investors and the assets under management of the investment manager do not exceed 100 million Swiss francs or 500 million Swiss francs and the investments do not include leveraged financial instruments, the respective investment manager is exempt from the licensing requirement under the FinIA.

Peer-to-peer and marketplace lending

9 | Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Swiss law does not provide for specific regulations applicable to peer-to-peer or marketplace lending. However, to the extent that a company operating a lending platform accepts and forwards funds committed to the platform, the operating fintech company is typically subject to the AMLA and the requirements set out thereunder, such as the duty:

- to become a member of a self-regulatory organisation;
- to determine the identity of the contracting party and the beneficial owner of the transferred assets; and
- to clarify the financial background and purpose of the business relationship or transaction, if the financial intermediary becomes aware of indications that the funds in question were obtained through criminal activities or are intended to finance terrorism.

Further, if loans are granted to consumers over the platform, the loans will be subject to the Federal Act on Consumer Credits and the fintech company operating the platform may – depending on the specific set-up – qualify as an arranger of consumer credits, requiring a licence under the CCA.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

Crowdfunding is not subject to specific legislation in Switzerland but is governed by the general Swiss financial market laws. In its fact sheet on crowdfunding FINMA provided

guidance on the regulatory treatment of crowdfunding platforms. Pursuant to FINMA's guidance, as a general rule, crowdfunding platforms are not subject to a licensing requirement in Switzerland, if the platform operator does not accept and channel the funds through its own accounts. In contrast, to the extent that the operator of a crowdfunding platform accepts funds exceeding 1 million Swiss francs (below such threshold the operator is exempt from the licensing requirement), rather than forwarding them to the borrower within 60 days and in consequence holds such funds in its own account for a longer period (for instance, to ensure that the amount is available at the end of a lengthy financing period), the operator is deemed to be engaging in regulated deposit-taking requiring a banking licence under the FBA. To the extent the funds do not exceed 100 million Swiss francs and such deposits are neither invested nor interest-bearing, the crowdfunding platform can be operated under a fintech licence pursuant to the FBA. In addition to potential licensing requirements, provided the platform operator channels funds through its accounts, the operator will be engaging in financial intermediation, subject to the Swiss anti-money laundering framework. Finally, it should also be noted that an entity raising funds for its own account over a crowdfunding platform may – depending on the specific set-up – be deemed to be accepting deposits within the meaning of the FBA. To the extent that the outstanding loans exceed 1 million Swiss francs, the borrower under a crowdfunding platform, accepting funds from numerous lenders, may be subject to the licensing requirements stipulated under the FBA.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

Invoice trading and factoring is not specifically regulated in Switzerland. Invoice trading and factoring generally do not require a licence under the financial market laws of Switzerland. In addition, invoice trading is generally not deemed to constitute financial intermediation subject to the Swiss anti-money laundering framework, whereas it will have to be determined on a case-by-case basis whether the underlying and acquired claims results from an activity subject to Swiss anti-money laundering regulations.

Payment services

12 | Are payment services regulated in your jurisdiction?

European Union Directive (EU) 2015/2366 (revised Payment Services Directive) is not applicable in Switzerland. Under the FMIA, an entity that operates a payment system (namely, a facility that clears and settles payment obligations based on uniform rules and procedures) is subject to a licensing requirement in Switzerland, provided:

- the licensing requirement is necessary for the proper functioning of the Swiss financial market or the protection of financial market participants; and
- the payment system is not operated by a licensed bank.

Licensed payment system providers are further subject to reporting obligations towards the Swiss National Bank (SNB). The SNB also has the regulatory powers to subject foreign payment systems that are of systemic relevance to Switzerland to its supervision. As a licensing requirement will only apply under the FMIA, to the extent a payment system is of systemic relevance in Switzerland, fintech companies providing payment services will

typically not be subject to a licensing requirement in Switzerland. However, the provision of payment services generally qualifies as financial intermediation subject to the Swiss anti-money laundering framework.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

Swiss law does not provide for specific regulations applicable to open banking. In Switzerland, open banking applications must adhere to the general banking secrecy, data protection and regulatory outsourcing requirements. While not widely applied and implemented in Switzerland, there are various industry initiatives monitoring the relevant developments. Notably, the Swiss Bankers Association has announced that it is actively monitoring the technical innovations in the open banking domain and intends to, together with market participants, contribute to the establishment of framework conditions that facilitate business models based on open banking and thus increase the competitiveness of Switzerland's financial centre.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

Swiss law does not provide for specific regulation applicable to robo-advisers, therefore, robo-advisers and the fintech companies operating such applications are subject to the general financial market laws in Switzerland. Whether or not a robo-adviser is subject to a licensing requirement in Switzerland depends on the specific activities performed and services offered by the robo-adviser. Typically, robo-advisers provide their services in cooperation with a licensed bank. Under such a set-up, the client will be onboarded by a third-party deposit bank holding the relevant client assets. The robo-adviser is then granted power of attorney over such assets to submit instructions to the relevant deposit bank to execute the transactions based on the automated investment decision rendered by the robo-adviser. In such a set-up, the robo-adviser will be rendering discretionary asset management services within the meaning of the FinIA. A robo-adviser, respectively the fintech company operating the robo-adviser, will, therefore, qualify as a regulated asset manager requiring a licence under the FinIA. In contrast, to the extent that the robo-adviser only provides investment advisory services (namely, by submitting investment proposals to the client based on its algorithms), the robo-adviser will not be subject to a licensing requirement in Switzerland. Both discretionary asset management and investment advice – depending on the specific set-up – qualify as a financial service within the meaning of the Federal Act on Financial Services (FinSA). As a consequence, the robo-adviser and the fintech company operating such robo-adviser will have to adhere to the ongoing conduct, client segmentation, documentation and organisational duties set out under the FinSA.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

The provision of insurance services in Switzerland requires a licence under the Federal Insurance Supervisory Act (ISA). The provision and the solicitation of insurance contracts and services is comprehensively regulated under the ISA. Therefore, for fintech and insurtech companies providing services under which the (monetary) risk in relation to certain events is transferred to a third party against the payment of a premium, it will have to be determined whether such services are subject to the ISA and the requirements set out thereunder.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

The provision of credit references or credit information is not specifically regulated under the laws of Switzerland and such services are generally not subject to a general regulatory licensing requirement. However, any company providing credit information must comply with the Swiss Federal Act on Data Protection, which applies not only to natural persons but also to legal entities. Further, the gathering of information from non-public sources may qualify as private detective services, which – depending on the specific set-up – may be subject to licensing requirements in certain cantons. Further, the cross-border provision of private detective services may trigger reporting obligations to the Swiss Foreign Department under the Federal Act on Private Security Services Abroad.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

No passporting of regulated activities into Switzerland is possible.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

The provision of financial services into Switzerland on a cross-border basis is not generally subject to a local presence requirement, with certain qualifications and exceptions depending on the types of regulated activities (eg, activities related to insurance and insurance brokerage; or the fact that the marketing of units in a foreign collective investment scheme to investors in Switzerland may require the appointment of a Swiss representative and a Swiss paying agent for that collective investment scheme).

At the level of prudential regulation, a foreign fintech company will generally require a Swiss licence only if it has a physical presence in Switzerland that exceeds certain de minimis thresholds.

At the level of conduct regulation, the provision of financial services within the meaning of the Federal Act on Financial Services as well as the marketing of collective investment schemes and structured products to clients or investors in Switzerland is a regulated activity even if carried on without a physical presence in Switzerland (subject to reverse solicitation and other exemptions) and may require the registration of client advisers in Switzerland.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

When marketing financial products, such as investment funds and structured products, the local Swiss rules on the marketing of such products must be complied with (eg, prospectus requirements under Swiss law).

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

While there are no general rules or regulations governing the use of distributed ledger technology or blockchains (and thus the general laws apply), on 25 September 2020, the Swiss Parliament approved the Law on Distributed Ledger Technology (the DLT Law). The DLT Law constitutes an 'umbrella legislation' that introduces a new concept of so-called 'DLT securities' under the Swiss Code of Obligations allowing for the tokenisation of rights, claims and financial instruments. In addition, the DLT Law provides for an introduction of a new licensing category – a DLT trading venue – under the Financial Market Infrastructure Act (FMIA) and certain clarifications relating to the treatment of cryptocurrencies in Swiss insolvency proceedings. The amendments to the Swiss Code of Obligations and the Federal Act on Intermediated Securities set out under the DLT Law, which enables the creation of ledger-based DLT securities, entered into force on 1 February 2021. Finally, during its meeting on 18 June 2021, the Swiss Federal Council enacted the remaining provisions of the DLT Law, which, together with the implementing ordinance, entered into force on 1 August 2021.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

As there are few specific rules or regulations governing the promotion or use of cryptoassets, the regulatory consequences depend on the nature of the asset and the activity.

First, an offer and sale of utility tokens, asset tokens and stablecoins may become subject to offer or sales regulations if the tokens in question constitute securities within the meaning of Swiss law. Sales activities relating to tokens that qualify as securities may in particular trigger:

- Swiss securities firm licence requirements under the Federal Act on Financial Institutions (FinIA);
- Swiss trading platform regulations under the FMIA; or
- Swiss prospectus requirements and further regulations in connection with financial services under the Federal Act on Financial Services (FinSA).

Under the Swiss Financial Market Supervisory Authority (FINMA) 'Guidelines for enquiries regarding the regulatory framework for initial coin offerings' of February 2018 and supplemented on 11 September 2019, the following three categories of tokens can be distinguished (even though tokens may also fall into more than one of these three basic categories):

- Payment tokens (pure cryptocurrencies): tokens that are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer. They do not give rise to any claims towards an issuer or a third party and to date are not treated as securities by the Swiss Financial Market Supervisory Authority (FINMA). The question of whether pure cryptocurrencies should nevertheless be treated as 'financial instruments' and as such subject to the regulation of financial services as set out in the FinSA remains unresolved (but given the wording of the FinSA, we believe that the question should be answered in the negative).
- Utility tokens: tokens that are intended to provide access digitally to an application or service by means of a DLT-based infrastructure. Subject to certain restrictions, utility tokens that neither fully nor partially serve investment purposes are currently not treated as securities by FINMA.
- Asset tokens: represent assets such as a debt or an equity claim against the issuer (such as a share in future company earnings or future capital flows). Being in terms of their economic function analogous to equities, bonds or derivatives, such tokens are generally treated as securities. Stablecoins and tokens that enable physical assets to be traded on a blockchain infrastructure may also fall into this category.

Second, and even with regard to cryptoassets that do not qualify as securities, a variety of regulatory licences may be relevant. In particular, only licensed banks are permitted to accept deposits from the public on a professional basis. Regulated deposit-taking may become an issue for service providers offering to store customers' cryptocurrencies, in particular. The new Swiss DLT Law has clarified under which circumstances the storage of cryptocurrencies requires a licence under the Federal Act on Banks and Savings Institutions,

such as a (simplified) fintech licence if the relevant cryptoassets assets are neither invested nor interest-bearing. Moreover, for crypto-based assets that banks hold as deposit assets for custodian clients, FINMA may set a maximum amount on a case-by-case basis if this appears necessary due to the risks associated with such business. Stablecoins in particular must, in the absence of more specific guidance from FINMA, be analysed on a case-by-case basis to determine whether any such licence (in particular, a banking or a securities firm licence, a payment system licence or a licence in connection with collective investment schemes) is required. Design features of stablecoins that may be decisive for whether a particular licence is required include:

- whether a single underlying or a basket of underlying is used;
- the type of underlying; and
- if the stablecoin in question gives the holder a contractual redemption claim with regard to the underlying, respectively, the value of the underlying, or if the token merely fulfils the function of evidencing an ownership position with regard to the underlying.

As a third factor, the Federal Anti-Money Laundering Act (AMLA) and its implementing regulations provide for a series of obligations that financial intermediaries must adhere to; for example, regarding the verification of the identity of customers or contracting parties as well as the beneficial owners of funds held.

With regard to cryptocurrencies, the following is important concerning anti-money laundering regulations:

- primary market initial coin offerings: according to FINMA, issuing cryptocurrencies (eg, payment tokens or stablecoins) constitutes financial intermediation (issuance of a means of payment); and
- secondary market sales and trading: merely selling cryptocurrencies to another party, or using such cryptocurrencies as means of payment for the sale or purchase of goods and services, does not constitute financial intermediation.

The revised Swiss Anti-Money Laundering Ordinance clarifies that the assistance provided in connection with the transfer of virtual currencies are services related to payment transactions that cause the service provider to be deemed a financial intermediary subject to the AMLA if such services are provided in the context of a permanent business relationship.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

As there are few specific rules or regulations governing the issuance of tokens, the regulatory consequences depend on the nature of the asset and the activity.

In particular, an offer and sale of utility tokens, asset tokens and stablecoins may become subject to offer or sales regulations if the tokens in question constitute securities within the meaning of Swiss law. Sales activities relating to tokens that qualify as securities may, in particular, trigger:

Read this article on Lexology

- Swiss securities firm licence requirements under the FinIA;
- Swiss trading platform regulations under the FMIA; or
- Swiss prospectus requirements and further regulations in connection with financial services under the FinSA.

Under FINMA's 'Guidelines for enquiries regarding the regulatory framework for initial coin offerings' of February 2018 and supplemented on 11 September 2019, the following three categories of tokens can be distinguished (even though tokens may also fall into more than one of these three basic categories):

- Payment tokens (pure cryptocurrencies): tokens that are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer. They do not give rise to any claims towards an issuer or a third party and to date are not treated as securities by the Swiss Financial Market Supervisory Authority (FINMA). The question of whether pure cryptocurrencies should nevertheless be treated as 'financial instruments' and as such subject to the regulation of financial services as set out in the FinSA remains unresolved (but given the wording of the FinSA, we believe that the question should be answered in the negative).
- Utility tokens: tokens that are intended to provide access digitally to an application or service by means of a DLT-based infrastructure. Subject to certain restrictions, utility tokens that neither fully nor partially serve investment purposes are currently not treated as securities by FINMA.
- Asset tokens: represent assets such as a debt or an equity claim against the issuer (such as a share in future company earnings or future capital flows). Being in terms of their economic function analogous to equities, bonds or derivatives, such tokens are generally treated as securities. Stablecoins and tokens that enable physical assets to be traded on a blockchain infrastructure may also fall into this category.

In addition, the AMLA and implementing regulations provide for a series of obligations that financial intermediaries must adhere to; for example, regarding the verification of the identity of customers or contracting parties as well as the beneficial owners of funds held. In the context of the primary market or ICO, according to FINMA, issuing cryptocurrencies (eg, payment tokens or stablecoins) constitutes financial intermediation (issuance of a means of payment).

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

Switzerland currently does not have special rules regarding the application of artificial intelligence, in spite of a number of reports having been commissioned by the Federal Council (the Swiss federal government). Notable among these reports is the 2019 report Challenges of Artificial Intelligence, authored by the Interdepartmental Working Group on artificial intelligence. A 2022 report on artificial intelligence and international rules, authored by the Federal Department of Foreign Affairs, characterises the 2019 report as 'a reference point

for AI rules and standards', but notes that it took 'a somewhat different approach from the one emerging internationally, where the emphasis is on regulating AI as a technology and defining key horizontal legal requirements with broad substantive and personal scope', whereas 'the [2019] report adopts a more technology-neutral approach, and only suggests amendments to the law where these are needed for specific sectors and applications'.

Swiss law does not provide for specific regulation applicable to robo-advisers, therefore robo-advisers and the fintech companies operating such applications are subject to the general financial market laws in Switzerland. Whether or not a robo-adviser is subject to a licensing requirement in Switzerland depends on the specific activities performed and services offered by the robo-adviser. Typically, robo-advisers provide their services in cooperation with a licensed bank. Under such a set-up, the client will be onboarded by a third-party deposit bank holding the relevant client assets. The robo-adviser is then granted power of attorney over such assets to submit instructions to the relevant deposit bank to execute the transactions based on the automated investment decision rendered by the robo-adviser. In such a set-up, the robo-adviser will be rendering discretionary asset management services within the meaning of the Federal Act on Financial Institutions (FinIA). A robo-adviser, respectively the fintech company operating the robo-adviser, will therefore qualify as a regulated asset manager requiring a licence under the FinIA. In contrast, to the extent that the robo-adviser only provides investment advisory services (namely, by submitting investment proposals to the client based on its algorithms), the robo-adviser will not be subject to a licensing requirement in Switzerland. Both discretionary asset management and investment advice – depending on the specific set-up – qualify as a financial service within the meaning of the Federal Act on Financial Services (FinSA). As a consequence, the robo-adviser and the fintech company operating such robo-adviser will have to adhere to the ongoing conduct, client segmentation, documentation and organisational duties set out under the FinSA.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

The regulatory requirements on Swiss-licensed financial institutions generally include that the natural and legal persons who directly or indirectly hold at least 10 per cent of capital or voting rights or exercise decisive influence on their business activities by other means ensure that their influence is not exercised to the detriment of prudent and sound management. The requirement for these financial institutions to meet the licensing requirements on an ongoing basis also means that almost all transactions involving significant changes in shareholders require Swiss Financial Market Supervisory Authority (FINMA) approval to be obtained. In addition, banks and securities firms organised under Swiss law but subject to a controlling foreign influence are subject to additional licensing requirements.

Shareholders in Swiss-licensed financial institutions may also be required to notify FINMA if their holdings cross or meet certain thresholds.

Read this article on Lexology

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Under Swiss law, both issuing cryptocurrencies as well as the subsequent trading of such tokens may be subject to anti-money laundering regulations.

The relevant starting point is to ask whether a person or company engages in any activities that constitute financial intermediation and is hence considered a financial intermediary under the Federal Anti-Money Laundering Act (AMLA). Other than licensed financial institutions, financial intermediaries include any persons or companies that, on a professional basis:

- accept or hold deposit assets belonging to third parties;
- assist in the investment of such assets; or
- assist in the transfer of such assets.

Prior to engaging in financial intermediation, such persons or companies that are not licenced financial institutions must join a Swiss self-regulatory organisation.

The AMLA and implementing regulations provide for a series of obligations that financial intermediaries must adhere to (eg, regarding the verification of the identity of customers or contracting parties as well as the beneficial owners of funds held).

With regard to cryptocurrencies, the following is important concerning anti-money laundering regulations:

- Primary market initial coin offerings: according to the Swiss Financial Market Supervisory Authority (FINMA), issuing cryptocurrencies (eg, payment tokens or stablecoins) constitutes financial intermediation (issuance of a means of payment).
- Secondary market sales and trading: merely selling cryptocurrencies to another party, or using such cryptocurrencies as means of payment for the sale or purchase of goods and services, does not constitute financial intermediation. The revised Swiss Anti-Money Laundering Ordinance clarifies that the assistance provided in connection with the transfer of virtual currencies are services related to payment transactions that cause the service provider to be deemed a financial intermediary subject to the AMLA if such services are provided in the context of a permanent business relationship.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no specific regulatory or industry anti-financial crime guidance for all fintech companies. However, some general principles and specific requirements can be deduced from interpretative guidance provided by the Federal Council (the Swiss federal government)

Read this article on Lexology

and FINMA as regards the interpretation and application of certain aspects of Swiss laws and regulations. For banks, the Swiss Bankers Association has issued guidelines on opening corporate accounts for distributed ledger technology companies that are binding on its members. The Capital Markets and Technology Association, an independent association, has also produced a set of 'AML Standards for Digital Assets'.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

In Switzerland, the Federal Act on Data Protection (DPA) and its corresponding ordinances regulate the processing of personal data by private parties. Thus, in relation to fintech products and services, the DPA includes the relevant rules and regulations governing the processing and transfer of personal data relating to such products and services. There are no sector-specific data protection rules specifically focusing on fintech products and services. However, where such products or services are offered by certain regulated businesses (eg, by banks, securities firms, financial markets infrastructure providers), in addition to general data protection law, specific confidentiality obligations may apply.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

In principle, the standard set by the DPA applies, which requires that those who process personal data implement and maintain adequate technical and organisational measures to ensure data security (namely, to prevent unauthorised processing of such personal data).

In addition, for certain regulated businesses, additional requirements under applicable financial markets regulation apply: for instance, banks are currently subject to Swiss Financial Market Supervisory Authority (FINMA) Circular 2008/21 on Operational Risks, which stipulates certain requirements applicable to electronic client data; effective as of 1 January 2024, this Circular 2008/21 will be replaced by the new FINMA Circular 2023/1 on Operational Risks and Resilience addressing also cyber risk and critical data risk management. In addition, FINMA has issued Guidance 05/2020 detailing FINMA's expectations in relation to the reporting of cyberattacks by supervised financial institutions.

Read this article on Lexology

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Outsourcing by banks, insurers and certain other regulated businesses is regulated by the Swiss Financial Market Supervisory Authority (FINMA) Circular 2018/3 on Outsourcing. This Circular defines the supervisory requirements that apply when a bank, insurance company or another regulated business within the scope of the Circular outsources a function that is significant to the company's business independently and on an ongoing basis. In addition to these specific requirements as per the Circular, general data protection law as well as the confidentiality obligation need to be taken into account. Where the outsourcing provider acts as a data processor for the financial services company, a data processing agreement is to be put in place.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

There is no specific law or regulation governing the use of cloud computing in the financial services industry. The applicable legal requirements follow from confidentiality obligations applicable in the financial services industry, namely:

- FINMA Circular 2018/3 on Outsourcing;
- FINMA Circular 2008/21 on Operational Risks;
- FINMA Circular 2023/1 on Operational Risks and Resilience, effective from 1 January 2024; and
- general data protection law.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Software is automatically protected under copyright law in Switzerland if and to the extent it constitutes a copyrightable work (namely, if it is an intellectual creation with individual character). Thus, there is no need for the author of the software to register the software or apply for protection to obtain copyright. In addition, patent protection is in principle also available for computer-implemented inventions where the necessary requirements are met. In any case, the abstract algorithm and basic idea underlying a computer software cannot be monopolised by copyright or patent protection.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Ownership belongs to the employer by way of statutory law where an employee, in performing work for the employer and complying with their duties under the employment contract, creates an invention or a design or computer software. Beyond that, the employer and the employee may agree for additional intellectual property rights to transfer to the employer by way of contract. In practice, it is advisable for an employment contract to specifically address the transfer of intellectual property created by the employee in the context of the employment relationship with the employer. There are no express corresponding rules applicable to third-party contractors and consultants, such that the ownership of the intellectual property created by such third parties would have to be determined in view of the specific circumstances. Thus, in practice, it is advisable to put in place a clear contractual arrangement.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Joint ownership is frequently discussed in contract negotiations, but most often not an ideal solution given that Switzerland, like many other jurisdictions, lacks explicit rules governing joint ownership of intellectual property. Thus, whenever that is contemplated, it is advisable to agree on joint ownership only based on a clear contractual basis governing each joint owner's right to use, license, charge or assign the relevant intellectual property or the ownership interest of such joint owner.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Trade secrets are protected under various statutory laws, including employment law, unfair competition law and criminal law. The relevant provisions limit the unlawful disclosure and exploitation of trade secrets. In addition, contractual confidentiality agreements serve to protect the confidentiality of trade secrets. In court proceedings, the court may upon request of a party impose measures to protect the confidentiality of trade secrets disclosed during the proceedings.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Trademark protection is available to protect branding. To obtain trademark protection, the relevant designation – for example, a word or logo, or a combination – must be filed as a trademark application to the Swiss Federal Institute of Intellectual Property. In addition to trademark protection, brands may also be protected under unfair competition law, which prohibits certain deceptive practices in commerce. It is advisable to conduct a proper search prior to adopting a brand to minimise the risk of infringing pre-existing trademark rights.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

In general, civil law remedies and criminal law remedies may be available to individuals or companies whose intellectual property rights have been infringed. Civil law remedies include actions to cease and desist from the infringing activities, compensation of damage and surrender of profits. In addition, infringements of intellectual property rights generally also constitute criminal offences, such that an individual or company whose intellectual property rights have been infringed may also file criminal complaints.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

The general competition law rules in Switzerland also apply to fintech companies and the fintech sector. Hence, fintech companies are subject to the general rules on prohibition of anticompetitive agreements, abuse of dominance and merger control. There are no sector-specific competition law rules targeting the fintech sector.

There has been certain enforcement action in the fintech sector in past years. With regard to anticompetitive agreements, the Swiss Competition Commission (ComCo) concluded an amicable settlement with Apple in 2018, according to which, Apple Pay shall not automatically start if a customer attempts to pay with the (competing) Swiss payment app TWINT. Following a complaint from Apple, ComCo is currently investigating an alleged boycott of Apple Pay by the Swiss banks (in favour of TWINT). With regard to abuse of dominance, ComCo has fined payment systems operator SIX approximately 7 million Swiss francs, in particular for refusal to supply interoperability information to competing payment terminal suppliers; the decision has been confirmed by the Federal Supreme Court in 2022. In the area of merger control, ComCo has approved the acquisition of joint control by SIX and

PostFinance over payment app TWINT subject to commitments that TWINT will not discriminate or grant exclusivities to other companies.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

There are no tax incentives created specifically for fintech companies in Switzerland. However, companies benefit from an attractive tax environment with low corporate tax rates (depending on the location within Switzerland), tax-free capital gains on the sale of equity investments by private individuals and lowered tax rates for the sale of substantial equity investments by legal entities. Private individuals also benefit from the tax exemption of capital gains on the sale of cryptocurrencies, creating an attractive market for a variety of different business models. The value added tax rate of 7.7 per cent is another locational advantage as it is quite low compared to most EU countries. Some fintech business models may even profit from a value added tax exemption if the offered services are similar to classic banking services (eg, brokering or granting of loans, brokerage or acceptance of deposits).

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

There are no tax changes planned that could hinder the development of fintechs. Rather, Switzerland will soon vote on the abolition of withholding taxes on bond interest payments. This has the potential to make bond financing in Switzerland more attractive for companies, but it also increases the attractiveness of different types of financing with bond-like characteristics (eg, issuing asset-backed tokens that qualify as debt financing).

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

There are no special immigration schemes available for fintech businesses or regimes specific to the technology or financial sector. However, citizens of EU member states are entitled to receive a work permit in Switzerland under the bilateral agreements between Switzerland and the European Union. Further, Switzerland and the United Kingdom are discussing a treaty to ensure that UK and Swiss nationals will continue to benefit from the privileges granted to EU member state citizens after Brexit. Nationals of a country outside

Read this article on Lexology

the European Economic Area will require a work permit, which may be subject to quotas. As a rule, work permits for highly qualified persons, such as senior managers or technical experts, will always be available.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

With the Law on Distributed Ledger Technology having entered into effect and additional amendments having been made to the Federal Act on Banks and Savings Institutions and Federal Anti-Money Laundering Act, clarifying the regulatory treatment of digital assets in Switzerland, the Swiss government has established a robust legal framework under which fintech companies are able to implement their respective business models. Under the Swiss legal framework, fintech companies can benefit from increased legal certainty, facilitating the provision of fintech-driven financial services.

While traditional financial service providers have more recently expanded their offerings to digital assets, a number of fintech companies have successfully entered the market for financial services in Switzerland. These developments and trends are expected to continue, with more and more decentralised finance applications expanding their offerings in Switzerland.

Homburger

Luca Dal Molin	luca.dalmolin@homburger.ch
Daniel Haeberli	daniel.haeberli@homburger.ch
Stefan Oesterhelt	stefan.oesterhelt@homburger.ch
Richard Stäuber	richard.staeuber@homburger.ch
Manuel Baschung	manuel.baschung@homburger.ch
Alexander Wherlock	alexander.wherlock@homburger.ch

Prime Tower, Hardstrasse 201, Zurich 8005, Switzerland
Tel: +41 43 222 1000
www.homburger.ch

Read more from this firm on Lexology

Read this article on Lexology

Taiwan

Abe T S Sung and Eddie Hsiung
Lee and Li Attorneys at Law

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 574
General innovation climate 574
Government and regulatory support 575

FINANCIAL REGULATION 575
Regulatory bodies 575
Regulated activities 576
Consumer lending 577
Secondary market loan trading 577
Collective investment schemes 577
Alternative investment funds 578
Peer-to-peer and marketplace lending 578
Crowdfunding 579
Invoice trading 580
Payment services 580
Open banking 581
Robo-advice 582
Insurance products 583
Credit references 583

CROSS-BORDER REGULATION 583
Passporting 583
Requirement for a local presence 583

SALES AND MARKETING 584
Restrictions 584

CRYPTOASSETS AND TOKENS 584
Distributed ledger technology 584
Cryptoassets 584
Token issuance 585

ARTIFICIAL INTELLIGENCE 587
Artificial intelligence 587

CHANGE OF CONTROL 587
Notification and consent 587

Read this article on Lexology

FINANCIAL CRIME 588
Anti-bribery and anti-money laundering procedures 588
Guidance 589

DATA PROTECTION AND CYBERSECURITY 589
Data protection 589
Cybersecurity 589

OUTSOURCING AND CLOUD COMPUTING 590
Outsourcing 590
Cloud computing 590

INTELLECTUAL PROPERTY RIGHTS 591
IP protection for software 591
IP developed by employees and contractors 592
Joint ownership 592
Trade secrets 593
Branding 593
Remedies for infringement of IP 593

COMPETITION 595
Sector-specific issues 595

TAX 595
Incentives 595
Increased tax burden 596

IMMIGRATION 596
Sector-specific schemes 596

UPDATE AND TRENDS 596
Current developments 596

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Taiwan's law for the fintech regulatory sandbox, the FinTech Development and Innovation and Experiment Act (the Sandbox Act) was promulgated on 31 January 2018 and took effect on 30 April 2018. As of June 2022, nine applications have been approved by the Financial Supervisory Commission (FSC) to enter into the sandbox, as summarised:

- to facilitate digital banking business (eg, online credit (credit card, credit facility)) by means of a mobile phone identity verification system;
- the outbound remittance by foreign workers through local convenience stores (two cases);
- to use blockchain technology for the transmission of fund transfer information between financial institutions;
- to enable customers to purchase travel insurance through the website of a travel agency by means of application programming interface connections;

Read this article on Lexology

- to provide the 'fund exchange' service by means of blockchain technology;
- to shorten the fund transmission gap by means of the 'T+0 contract mechanism';
- to provide a group buying platform for investing in bonds with blockchain as the underlying technology; and
- to allow investors to buy US exchange-traded funds using a US dollar cost-averaging strategy based on the advice provided by robo-advisers.

According to relevant local news reports and the FSC website, some of the applications that entered the regulatory sandbox are now existing practices, while some may be implemented legally in the near future. Generally speaking, applicants of experiments under the Sandbox Act may apply for the new licence or approval for their business once the existing laws and regulations involved in the experiments have been amended by the FSC or the Legislative Yuan.

In addition to the sandbox mechanism described above, in 2018, the Taiwan government also supported fintech developments by, for example, establishing the FinTechSpace, which is a physical location situated in the city of Taipei with an aim to provide relevant assistance to fintech start-ups, such as acting as an intermediary between fintech start-ups and financial services entities (with respect to potential cooperation between the parties), a regulatory clinic (namely, free preliminary advice provided by government officials regarding regulations), etc.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

The regulatory sandbox offers a platform to test new applications of fintech technologies. According to the Sandbox Act, an applicant (who can be an entity or individual) needs to obtain an approval from the FSC before entering the sandbox and beginning the experiment. During the experiment period, the experimental activities may enjoy exemptions from certain laws and regulations (such as FSC licensing requirements and certain legal liability exemptions). After completion of the approved experiments, the FSC will analyse the results of them. If the result is positive, the FSC may review the existing financial laws and regulations and explore the possibility of amending the existing rules that pose obstacles to the experimented financial innovation if put in the real world. However, depending on the review result of the FSC, the sandbox entity or individual might still be required to apply for a relevant licence or approval from the FSC to formally conduct the activities as previously tested in the sandbox.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

In Taiwan, the Financial Supervisory Commission (FSC) is the government body regulating all financial products and services. There are four bureaux established under the FSC:

- the Banking Bureau (BB);
- the Securities and Futures Bureau (SFB);
- the Insurance Bureau (IB); and
- the Financial Examination Bureau (EB) (collectively the Bureaux).

Each of the BB, SFB and IB is separately responsible for regulating the banking, securities and insurance industries. The EB is in charge of financial inspection and audits of financial institutions regulated by the FSC. Currently, none of the four bureaux has been specifically designated to regulate fintech products and services. Therefore, it should depend on the nature of such products and services to determine which bureau would be the body regulating the relevant fintech products or services.

As to the mechanism of the regulatory sandbox, the FSC is the competent authority; nonetheless, if the tested fintech product and service relates to the regulatory regime of other competent authorities (such as the Central Bank), the opinion of these relevant authorities will also be consulted by the FSC.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

In Taiwan, conducting finance-related activities generally requires a licence from the FSC. These activities include the following, without limitation.

- Securities-related activities: securities underwriting, securities brokerage, securities dealing (ie, proprietary trading), securities investment trust (ie, asset management) and securities investment consulting.
- General consulting business, such as acting as financial advisers or agents to arrange investments or bring about merger or acquisition deals, does not require any licence. In addition, acting as principal in an investment deal does not require any licence (except if a foreign investor should need a foreign investment approval and investment in regulated industries needs special approvals).
- Bank-related activities:
    - lending: lending activities do not fall within the business to be exclusively conducted by a local licensed bank. However, as no financing company may be registered in Taiwan, it is currently not possible for an entity to register as a financing company to carry on lending activities in Taiwan;
    - factoring and invoice, discounting and secondary market loan trading;
    - deposit-taking;
    - foreign exchange trading;
    - remittance; and
    - electronic payment, credit cards and electronic stored-value cards.

Consumer lending

5 Is consumer lending regulated in your jurisdiction?

A local licensed bank may carry on consumer lending activities. Although lending activities do not fall within the business to be exclusively conducted by a local licensed bank, carrying out lending activities as one of a company's registered business activities is still not permitted in Taiwan.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

The general principle under Taiwan's Civil Code is that any receivable is assignable unless:

1 the nature of the receivable does not permit this transfer;
2 the parties to the loan have agreed that the receivable shall not be transferred; or
3 the receivable, in nature, is not legally attachable.

The receivables under a loan, subject to (2), are generally transferable. However, a bank is subject to stricter rules that, generally, loans that remain performing cannot be transferred by a bank, with some limited exceptions (such as for the purpose of securitisation). For this reason, Taiwan does not currently have an active secondary loan market.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Local funds (securities investment trust funds)

The most common form of collective investment scheme in Taiwan is securities investment trust funds, which may be offered to the general public or privately placed to specified persons. Public offering of a securities investment trust fund needs prior approval or effective registration with the FSC or the institution designated by the FSC. No prior approval is required for a private placement of a securities investment trust fund; however, it can only be placed to eligible investors and within five days after the payment of the subscription price for initial investment offering, a report on the private placement shall be filed with the FSC or the institution designated by the FSC. Generally, the total number of qualified non-institutional investors under a private placement shall not exceed 99. Under current laws and regulations, public offering and private placement of securities investment trust funds may only be conducted by FSC-licensed securities investment trust enterprises (SITEs). Currently, the paid-in capital of a SITE should not be lower than NT$300 million, and there exist certain qualifications for the shareholders of a SITE. A fintech company, which is not a SITE, will not be able to raise funds as a SITE does.

Offshore funds

Offshore funds with the nature of a securities investment trust fund may also be publicly offered (subject to FSC prior approval) or privately placed (subject to post-filing with the FSC or its designated institution) to Taiwan investors, subject to certain qualifications and conditions. An offshore fintech company, which does not have the nature of a securities investment trust fund, will not be allowed to be offered in Taiwan.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Currently, only securities investment funds, real property trust funds and futures trust funds (which focus on investment in futures and derivatives) are permitted in Taiwan (except that SITEs and securities firms are now permitted to set up a subsidiary to act as the general partner of a private equity fund under the structure of limited partnership). These funds may only be offered and managed by FSC-licensed entities, such as SITEs, banks or futures trust enterprises. A fintech company, which is not a SITE, a bank or a futures trust enterprise, will not be allowed to manage these funds in Taiwan.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

While to date there are no laws or regulations specifically regulating or governing peer-to-peer lending, the Bankers Association of the Republic of China (the Bankers Association), the self-disciplinary organisation of the banking industry, has promulgated the Self-Disciplinary Rules of Business Cooperation between Member Banks of Bankers Association and Peer-to-Peer Lending Operators (the P2P Self-Disciplinary Rules) and such P2P Self-Disciplinary Rules have been filed with the FSC for the record.

According to the P2P Self-Disciplinary Rules, banks may work together with peer-to-peer lending operators on the following matters:

- providing fund custodian services;
- providing cash-flow services;
- providing credit review and rating services;
- extending facility by a bank to the customer (ie, the people-to-business model);
- advertising and marketing activities; and
- providing credit document custody services.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

Equity-based crowdfunding

The following two ways of fundraising are generally known as equity-based crowdfunding platforms in Taiwan. These ways of crowdfunding are exempted from the prior approval or effective registration normally required under the Securities and Exchange Act (SEA).

The Go Incubation Board for Startup and Acceleration Firms of the Taipei Exchange

The Taipei Exchange (TPEx), one of the two securities exchanges in Taiwan, established the Go Incubation Board for Startup and Acceleration Firms (GISA) in 2014 for the purpose of assisting innovative and creative small non-public companies in capital raising.

A company with innovative or creative ideas with the potential for development is qualified to apply for GISA registration with the TPEx. After the TPEx approves the application, the company will first start receiving counselling services from the TPEx regarding accounting, internal control, marketing and legal affairs. After the counselling period, there is another TPEx review to examine, among other things, the company's management teams, the role of the board of directors, accounting and internal control systems, and the reasonableness and feasibility of the plan for raising capital, and if the TPEx deems appropriate, the company may raise capital on the GISA. The amount raised by the company through the GISA may not exceed NT$30 million unless otherwise approved. In addition, an investor's annual maximum amount of investment through the GISA should not exceed NT$150,000, except for in the case of angel investors defined by the TPEx or wealthy individuals with assets exceeding an amount set by the TPEx and with professional knowledge regarding financial products or trading experience.

Equity-based crowdfunding on the platforms of securities firms

A securities firm may also establish a crowdfunding platform and conduct an equity crowdfunding business. Currently, a company with paid-in capital of less than NT$50 million may enter into a contract with a qualified securities firm to raise funds through the crowdfunding platform maintained by the securities firm, provided that the total amount of funds raised by the company through all securities firms' crowdfunding platforms in a year may not exceed NT$30 million. The amount of investment made by an investor on a securities firm's platform may not exceed NT$150,000 in aggregate in a year, except for in the case of:

1 a natural person who provides proof of financial resources of at least NT$ 30 million and has sufficient expertise or experience in financial instruments;
2 the directors, supervisors and shareholders holding more than 10 per cent of the shares of the company; and
3 angel investors as defined in the relevant regulations.

Non-equity-based crowdfunding

In 2013, the TPEx established the Gofunding Zone on its official website. This mechanism allows the non-equity-based crowdfunding platform operators, once approved by the TPEx, to post information regarding their proposals and projects on the Gofunding Zone. However, in May 2018, the TPEx announced that owing to the significant developments in the crowd-funding business, the phased task of the TPEx to support this business had been completed, and, thus, it decided to close the Gofunding Zone and annulled relevant rules.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

The general principle under Taiwan's Civil Code is that any receivable is assignable unless:

1 the nature of the receivable does not permit this transfer;
2 the parties to the loan have agreed that the receivable shall not be transferred; or
3 the receivable, in nature, is not legally attachable.

The receivables under a loan, subject to (2), are generally transferable. However, a bank is subject to stricter rules that, generally, loans that remain performing cannot be transferred by a bank, with some limited exceptions (such as for the purpose of securitisation).

In general, no company may carry out the activities of receivable transfer for business. Purchase of accounts receivable may only be conducted by a licensed bank.

Payment services

12 | Are payment services regulated in your jurisdiction?

Payments using the services of a licensed bank

Yes. Traditionally payments by wire transfer can only be made through a licensed bank. Payments via cheques and credit cards are also run through banks.

E-payment institutions

The Electronic Payment Institutions Act (the E-payment Act), which governs the online payment sector in Taiwan, was enacted in 2015. In December 2020, Taiwan's parliament, the Legislative Yuan, made an amendment to the E-payment Act, which took effect on 1 July 2021. Under the amended E-payment Act, the scope of business of a new e-payment institution will include core businesses and ancillary and derivative businesses.

For the core businesses, in addition to the existing businesses of:

- collecting and making payments for real transactions as an agent; and
- accepting deposits of funds as stored value funds.

The new business small amount domestic and cross-border remittance services and foreign exchange services relating to the core businesses will also be opened to e-payment institutions from the effective date of the amendment.

The ancillary and derivative businesses are all new under the E-payment Act, which include:

- assisting the contracted merchants with integration and transmission of acquiring and payment information;
- sharing terminal equipment at the contracted merchants;
- assisting the information exchange between the users and between the users and the contracted merchants;
- providing an electronic uniform invoice system and its value-added services;
- taking custody of paid price of vouchers or tickets of goods or services, and assisting in the issuance, sales, validation and related services for vouchers or tickets;
- providing services for integration of bonus points and offsetting or settling payments for real transactions with bonus points;
- providing value-storing blocks in electronically stored value cards or application programmes for use by others; and
- providing any planning, instalment, maintenance or consultancy services for the information system and facilities in relation to the above seven ancillary and derivative businesses of e-payment institutions.

'Small amount remittances by foreign workers' allowed for non-payment institutions

The amended E-payment Act would also permit qualified non-e-payment institutions to apply to become cross-border remittance service providers exclusively for foreign workers in Taiwan. Detailed enforcement rules and regulations have also been promulgated by the FSC and took effect on 1 July 2021.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

While the FSC has the general power to request the provision of customer or product data by financial institutions to the FSC, in practice, the FSC's relevant regulations, directions or guidelines also require that financial institutions provide relevant customer and product data (such as data relating to credit extensions, credit cards and derivatives) to the Joint Credit Information Center (JCIC) for banks' use of credit check in terms of credit extension.

In addition, in response to the advocacy of 'open banking' from some industry experts and market players, the FSC has demanded the Bankers Association set out relevant self-regulatory rules to implement the concept of open banking in Taiwan. The FSC did not wish to set out mandatory disclosure rules for banks, and instead, asked the self-regulatory organisation (ie, the Bankers Association) and the Financial Information Service Co to set out relevant rules and information security standards for banks to follow.

Read this article on Lexology

The FSC, as reported, adopts a three-phase approach to open banking. Phase I of 'open banking' was launched in late 2019, to allow public product information to be searchable by third parties (namely, third-party service providers (TSPs)). Phase II involves access to customer data. According to relevant FSC press releases, several TSPs have been approved by the FSC to collaborate with certain banks under Phase II. Phase III will involve the processing of transactions. It is generally perceived that the complexity and risk of releasing transaction data of customers involved in this Phase would increase, and therefore the technology to support, monitor and secure the open application programming interface access would be more complex and critical. For the same reason, the timeline to launch Phase III is still under discussion.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

In June 2017, the Securities Investment Trust and Consulting Association of Taiwan, the self-disciplinary organisation of the asset management industry, issued the Operating Rules for Securities Investment Consulting Enterprises Using Automated Tools to Provide Consulting Service (Robo-Advisor) (the Robo-Advisor Rules), which was approved by the FSC. Pursuant to the Robo-Advisor Rules, securities investment consulting enterprises may provide online securities investment consulting services by using automated tools through an algorithm (Robo-Advisor Services) and they must comply with certain rules, which include, among others, the following:

- periodical review of the algorithm;
- relevant know-your-customer procedures should be conducted before the provision of advice;
- a special committee should be established to supervise the adequacy of the Robo-Advisor Services; and
- customers should be informed of precautions before using Robo-Advisor Services.

With respect to the requirements of the Robo-Advisor's rebalancing transactions, the FSC, on 18 November 2021, further relaxed the restrictions where the investment portfolios agreed between the Robo-Advisor and its clients that securities investment trust funds or offshore funds (approved by or registered with the FSC) and the rebalancing transactions can be executed on the following conditions:

- it adheres to the funds' list agreed with the client in advance (up to 30 funds); and
- it aggregates absolute value of the change in the investment proportion of each investment portfolio which does not exceed 60 per cent.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

In Taiwan, selling insurance products will be considered conducting insurance business, which requires an insurance licence from the FSC. A fintech company is not permitted to sell any insurance products without an insurance licence from the FSC.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Yes. Pursuant to the Banking Act and relevant regulations, an entity collecting credit-related information from financial institutions, processing this information and maintaining the relevant database and providing credit-related information and records to financial institutions for credit-checking purposes must obtain prior approval from the FSC. Currently, the Joint Credit Information Center (JCIC) is the only FSC-authorised entity that offers these services. In practice, a bank would normally review the credit information or records provided by the JCIC as part of the bank's credit investigation on an applicant for a credit extension.

If an entity does not offer these services, no FSC approval is required, but it will still be subject to the Personal Data Protection Act regarding its collection and use of any personal data.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

There is no concept of passporting right in Taiwan. To engage in regulated financial activities, a company needs to apply for the relevant licences from the Financial Supervisory Commission (FSC). Depending on the types of regulated activities, the applicant must meet certain qualifications as required under relevant laws and FSC regulations.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

No. Foreign companies cannot carry on regulated business (which includes financial services) without a licence, and the FSC licences required for providing financial services are not issued to foreign companies without establishing a subsidiary or a branch in Taiwan.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

The Financial Consumer Protection Act (FCPA) and its related regulations provide for the general marketing rules applicable to the marketing materials for financial services. In general, under the FCPA, when carrying out advertising, promotional or marketing activities, financial services providers should not falsify, conceal, hide or take any action that would mislead financial consumers and they should ensure the truthfulness of the advertisements. In addition to the general marketing rules under the FCPA, the financial service providers may also be subject to additional marketing rules as specified in the laws and regulations governing the specific types of financial services or products.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

No.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

Digital currencies (such as virtual currencies or cryptocurrencies with the applications of blockchain technology) that are not linked or tied to the currency of any nation are currently not accepted by the Central Bank of the Republic of China (Taiwan) (the Central Bank) as currencies. In December 2013, both the Central Bank and the Financial Supervisory Commission (FSC) expressed the government's position toward bitcoin by issuing a joint press release (the 2013 Release). According to the 2013 Release, the two authorities held that bitcoin should not be considered a currency, but a highly speculative digital virtual commodity. In another FSC press release in 2014 (the 2014 Release), the FSC ordered that local banks must not accept bitcoin or provide any other services related to bitcoin (such as exchanging bitcoin for fiat currency). The FSC further issued a press release on 19 December 2017, in which it reiterated the government's positions as specified in the 2013 Release and 2014 Release. Other than the above, no laws, regulations or rulings have been officially issued, promulgated or amended to specifically deal with the rise of digital currencies, except for the regulations governing tokens that have the nature of securities.

With regard to stablecoins, the Central Bank released a report on 16 December 2021, warning that stablecoins are used to facilitate speculative trading and investment in virtual assets

Read this article on Lexology

and the price is not entirely stable as the prevalent circulation of stablecoins could cause inefficiencies in the function of price stabilisation mechanisms. The report further indicates that the issuance of stablecoins must comply with the related regulations governing electronic payment institutions, banks, etc, if the relevant activities fall within the scope of regulated activities under e-payment and banking laws.

With respect to NFTs (which have been commonly structured to represent digital artworks, music works, collectables, baseball and basketball cards, photo albums, etc), recent discussions have focused on what an NFT holder actually 'owns' or has 'obtained' in relation to an NFT. The classification of any NFT and its offering should also be examined on a case-by-case basis. Also, notwithstanding the nature of any NFT being 'non-fungible' and unique, we still cannot completely rule out the applicability of financial law (eg, securities regulations) due to the possible nature of investments.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

In response to the rising amount of ICOs and other investment activities regarding digital currencies and cryptocurrencies, the FSC also expressed the following views on ICO through a press release issued by FSC on 19 December 2017:

- The classification of an ICO should be determined on a case-by-case basis. If an ICO involves offer and issue of securities, it should be subject to the Securities and Exchange Act (SEA). The issue of whether tokens in an ICO would be deemed securities under the SEA would depend on the facts of each individual case.
- If any misrepresentations with respect to technologies or their outcomes or promises of unreasonably high returns are used by the issuer of virtual currencies or an ICO to attract investors, the issuer would be deemed as committing fraud or illegal fundraising.

On 3 July 2019, the FSC, by issuing a ruling, officially designated cryptocurrencies with the nature of securities (namely, security tokens, as 'securities' under the SEA (the 2019 Ruling)). According to the 2019 Ruling, security tokens refer to those that:

- utilise cryptography, distributed ledger technology or other similar technologies to represent their value that can be stored, exchanged or transferred through digital mechanism;
- are transferable; and
- encompass all of the following attributes of an investment:

    - funding provided by investors;
    - providing funding for a common enterprise or project;
    - investors expecting to receive profits; and
    - profits generated primarily from the efforts of the issuer or third parties.

In addition to the 2019 Ruling, the FSC issued a press release on 27 June 2019 to illustrate the key points of the FSC's policy on STOs. Since then, the FSC and the Taipei Exchange

(TPEx) have been setting out the regulations governing STOs (the STO Rules), and the STO Rules were finalised in January 2020. Specifically, the FSC differentiates the regulation of STOs with the threshold of NT$30 million. For an STO of NT$30 million or less, the STO may be conducted in compliance with the STO Rules; an STO above NT$30 million must first apply to be tested in the 'financial regulatory sandbox' pursuant to the FinTech Development and Innovation and Experiment Act and, if the experiment has a positive outcome, should be conducted pursuant to the SEA. Certain other major provisions of the STO Rules (namely, for STOs of NT$30 million or less) are set out in the following.

Regulations on issuance (primary market)

- Qualifications of the issuer: the issuer must be a company limited by shares incorporated under the laws of Taiwan and not a company listed on the TPEx or traded on the Emerging Stock Market. This indicates that a foreign entity may not act as an issuer of an STO programme.
- Types of security tokens that can be issued: the issuer can only issue profit-sharing or debt tokens without shareholder's rights, meaning that shares, being a type of security under the SEA, with regular shareholder's rights of an issuer cannot be issued in the form of security token while bonds can be issued as debt tokens.
- Eligible investors and amount limits: Apart from 'professional investors' who are eligible to participate in STOs; where the professional investor is a natural person, the maximum subscription amount is NT$300,000 per STO, to promote the development of STO, the FSC issued a press release in January 2022 (2022 press release) to adjust the policy and soon afterwards the TPEx amended the STO rules on 10 February 2022 to expand the scope of eligible foreign investors meeting certain criteria under the STO rules.
- Issuance process: issuers must conduct STOs on a single platform, and the platform operator has the obligation to ensure that the issuer meets the qualification requirements and that the prospectus is well prepared. Where the platform operator itself is an STO issuer, such issuer should not launch an STO without a prior review by TPEx.

Regulations on trading (secondary market)

- Trading mechanism for security tokens: the platform operator should obtain a securities dealer licence and handle the trading by way of price negotiation. The platform operator should be the counterparty to every transaction and should offer a reasonable reference quotation based on market conditions. In addition, each security token under an STO programme may be traded only on a single platform.
- Maximum transaction amount: where the professional investor is a natural person, the maximum amount of holding under an STO programme is NT$300,000. In addition, the maximum daily transaction limit for each STO is 50 per cent of the total issuance amount under such STO programme.

STO platform operator

- Qualifications of the platform operator: the platform operator should obtain a securities dealer licence, have minimum paid-in capital of NT$100 million and provide an operation bond of NT$10 million.
- Total offering amount capacity: the total offering amount of all STOs on a single platform should not exceed NT$200 million. A platform can accept to process a second STO only six months after the security tokens of the first STO have been traded on the platform without material violation of the relevant regulations during the period.

Read this article on Lexology

- Transfer and record keeping: the platform operator should enter into an agreement with the Taiwan Depository and Clearing Corporation (TDCC) and transmit the trading information such as balance changes and balance statements to the TDCC for its record on a daily basis. The TDCC should provide an STO balance inquiry service to investors.
- Subscription and trading: subscription and trading of security tokens should be conducted on a real-name basis and the transactions must be conducted in New Taiwan dollars under the same name as the account name of the bank account.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

The Taiwan government announced the 5+2 Industrial Innovation Plan (the 5+2 Plan) in 2008, in which artificial intelligence (AI) played an important role. The 5+2 Plan mainly focuses on seven industries (namely, intelligent machinery, Asia Silicon Valley, green energy, biomedicine, national defence and aerospace, new agriculture and the circular economy), and is considered the core generator for Taiwan's next generation of industrial development. To facilitate the 5+2 Plan, the government also launched the AI Talent Programme, which aims to:

- cultivate 1,000 high-calibre talents in intelligent technologies;
- train 5,000 talents in practical intelligent technologies; and
- attract foreign professionals.

The launch of ChatGPT has again set off a boom in the application of AI. According to relevant news reports, in response to the trend of AI developments, the Financial Supervisory Commission is contemplating including AI-related policy in its Financial Technology Development Program 2.0 to be announced in August 2023, as well as setting out relevant new rules and regulations to govern the use of AI in the financial services industry.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

The rules relating to notification or approval requirements for change of control of a financial services company vary among the types of companies. For example:

- bank: a prior approval must be obtained from the Financial Supervisory Commission (FSC) if an investor or its related parties has individually, jointly or collectively acquired or held more than 10, 25 or 50 per cent of the voting shares of a bank;
- securities firm: no prior approval from the FSC is required;

Read this article on Lexology

- securities investment trust enterprise (SITEs): if the professional shareholder of a SITE intends to transfer its shareholding in the SITE, the SITE should report to the FSC the transfer of shares before the transfer is conducted; and
- securities investment consulting enterprise: no prior approval from the FSC is required.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Money laundering activities are mainly regulated by the Money Laundering Control Act (MLCA) (last amended on 7 November 2018) and its related regulations. Under the MLCA, to prevent money laundering activities, financial institutions are required to implement their own internal anti-money laundering guidelines and procedures and submit them to the Financial Supervisory Commission (FSC) for the record.

With respect to digital currency platform operators or transactions, the latest amended MLCA has brought the 'virtual currency platforms and trading business' into Taiwan's AML regulatory regime, under which the enterprises falling within the designated scope would be subject to the relevant rules applicable to financial institutions under the MLCA. On 7 April 2021, Taiwan's Executive Yuan issued a ruling (the AML Ruling), interpreting the scope of enterprises of 'virtual currency platforms and trading business' under the MLCA, which took effect on 1 July 2021. The scope described under the AML Ruling covers those who engage in the following activities for others:

- exchange between virtual currency and New Taiwan Dollars, foreign currencies or currencies issued by mainland China, Hong Kong or Macao;
- exchange between virtual currencies;
- transfer of virtual currencies;
- custody and administration of virtual currency or providing instruments enabling control over virtual currencies; and
- participation in and provision of financial services related to the issuance or sale of virtual currencies.

After the AML Ruling was issued, the FSC promulgated the Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises of Virtual Currency Platforms and Trading Business. According to the regulations, the designated operators of crypto-assets and exchanges are required to establish, among other things, an internal control and audit mechanism, reporting procedure of suspicious transactions and the KYC procedure, etc. The regulations took effect on 1 July 2021, save for the provision requiring the 'transfer-out' of the cryptocurrency to be carried out on a no-name basis both for the transferor and transferee – the effective date of such provision will be further determined by the FSC.

Further, the FSC designated 'cross-border small-amount remittance' service providers exclusively for foreign workers in Taiwan to be 'financial institutions' under the MLCA on 9

August 2021; therefore, such providers will also be subject to the AML requirements applicable to financial institutions.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

No.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

In Taiwan, personal data is generally protected by the Personal Data Protection Act (PDPA). Under the PDPA, unless otherwise specified under law, a company is generally required to give notice to (notice requirement) and obtain consent from (consent requirement) an individual before collecting, processing or using any of this individual's personal information, subject to certain exemptions. To satisfy the notice requirement, certain matters must be communicated to the individual, such as the purposes for which his or her data is collected, the type of the personal data and the term, area and persons authorised to use the data.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

Different cybersecurity regulations or standards may apply to different types of financial service entities or their products or services. For example, if a type of fintech business is considered to fall within the scope of electronic banking business, in addition to the relevant licensing requirements under certain financial regulations, it should also comply with the rules governing the security control for this business.

With respect to the 'regulatory sandbox' under the FinTech Development and Innovation and Experiment Act, a relevant description regarding the information system and security control is required for an application for entering the sandbox.

The Cyber Security Management Act (CSMA) was enacted in June 2018. According to the CSMA, financial services firms would be required to comply with relevant obligations (including, among other things, requirements for meeting a specific security level, setting up relevant internal rules for implementing plans for maintaining information security and reporting to the government in the case of any cyber security incident) under the CSMA if they are designated by the Taiwan government as the 'critical infrastructure provider' (CIP) under the CSMA. While we think that no specific fintech business would be designated as a CIP, the CSMA would still apply to fintech businesses if the types of financial service

entities carrying out these fintech business activities are considered Financial Supervisory Commission-regulated entities and are designated as CIPs by the Taiwan government.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

The legal requirements with respect to outsourcing by a financial services company vary among the types of companies. For example, a bank's outsourcing must comply with the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation (the Banks' Outsourcing Regulations), under which only the activities enumerated in the Banks' Outsourcing Regulations can be outsourced (subject to relevant requirements such as supervision of the outsourced party and the contract with the outsourced party), and outsourcing of some activities would require prior approval from the Financial Supervisory Commission (FSC).

As for other financial services companies, for certain types of financial services companies, no single regulation exists that governs their outsourcing activities, so generally, outsourcing is allowed only if the FSC has issued any ruling permitting it. For example, a securities investment trust enterprise (SITE) is permitted to outsource its operation of evaluating fund assets, calculation of a fund's net worth and fund accounting to a professional institution, subject to applicable requirements specified under the relevant FSC rulings.

According to the Banks' Outsourcing Regulations, as last amended on 30 September 2019, prior approval from the FSC is required if a financial institution outsources an operation involving cloud-based services and the outsourcing is considered 'material' or the operation is outsourced to an overseas service provider. Further, when outsourcing involves cloud-based services, the financial institution shall, among other things:

- ensure appropriate diversification of cloud service providers;
- retain full ownership of the data outsourced to the cloud service provider; and
- ensure the location for processing and storage is within Taiwan (with certain exceptions).

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

When the use of cloud computing involves outsourcing the operations of a financial institution, relevant laws and regulations governing outsourcing activities should be complied with. In general, an outsourcing activity should follow the internal rules and procedures of the financial institutions, and in certain circumstances, prior approval from the FSC would be required. The use of cloud computing should also comply with the Personal Data Protection Act.

Read this article on Lexology

According to the Banks' Outsourcing Regulations, as last amended on 30 September 2019, prior approval from the FSC is required if a financial institution outsources an operation involving cloud-based services and the outsourcing is considered 'material' or the operation is outsourced to an overseas service provider. Further, when outsourcing involves cloud-based services, the financial institution shall, among other things:

- ensure appropriate diversification of cloud service providers;
- retain full ownership of the data outsourced to the cloud service provider; and
- ensure the location for processing and storage is within Taiwan (with certain exceptions).

It is noteworthy that the FSC announced that it plans to amend the Banks' Outsourcing Regulations. According to the relevant draft amendment, a Taiwanese bank would not be required to apply to the FSC to obtain its prior approval for all of the offshore outsourcing arrangements. Instead, only when a bank intends to outsource its business activities regarding the retail financial business information systems to an offshore service provider, and such outsourcing is deemed 'material', shall such bank apply to the FSC for its prior approval. According to the FSC's official press release, it expects to complete the amendments and put them into effect in September 2023, while when the amendments will become effective is still uncertain.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Software can be protected by intellectual property rights such as patent, copyright or trade secret. As to patent, an inventor may file an application with Taiwan's Intellectual Property Office, and the patent right will be obtained once the application is approved. For copyrights and trade secrets, there are no registration or filing requirements for a copyright or a trade secret to be protected by law. However, there are certain features that qualify a copyright or trade secret, such as 'originality' and 'expression' for copyrights, and 'economic valuable' and 'adoption of reasonable protection measures' for trade secrets.

According to the Patent Act of Taiwan, the subject of a patent right is 'invention' and an invention means the creation of technical ideas, utilising the laws of nature. As a general rule, business methods are regarded as using social or business rules rather than laws of nature, and therefore may not be the subject of a patent right. As for software-implemented inventions, if it coordinates the software and hardware to process the information, and there is a technical effect in its operation, it might become patentable. For instance, a 'method of conducting foreign exchange transaction' would be deemed as a business method and thus unpatentable; however, a 'method of using financial information system to process foreign exchange transactions' might be patentable.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Intellectual property developed by an employee during the course of employment

With regard to a patent, the right of an invention made by an employee during the course of performing his or her duties under employment will be vested in his or her employer and the employer should pay the employee reasonable remuneration unless otherwise agreed by the parties.

A trade secret is the result of research or development by an employee during the course of performing his or her duties under employment and it will belong to the employer unless otherwise agreed by the parties.

For copyright, where a work is completed by an employee within the scope of employment, the employee is the author of the work but the economic rights to this work will be enjoyed by the employer unless otherwise agreed by the parties.

Intellectual property developed by contractors or consultants

In respect of patent rights and trade secrets, the agreement between the parties will prevail, or these rights will be vested in the inventor or developer in the absence of such agreement. However, if there is a fund provider, the funder may use this invention.

In respect of copyright, the contractor or the consultant who actually makes the work is the author of the work unless otherwise agreed by the parties; the enjoyment of the economic rights arising from the work should be agreed by the parties, or these rights will be enjoyed by the contractor or the consultant in the absence of such agreement. However, the commissioning party may use the work.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

In respect of patents and trademarks, each joint owner may use the jointly owned rights at his, her or its discretion; however, a joint owner may not license or assign the jointly owned rights without consent of all the other joint owners. In respect of copyrights and trade secrets, each joint owner may not use, license or assign the rights without unanimous consent of the other joint owners, while the other joint owners may not withhold the consent without reasonable cause.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Trade secrets are protected if they satisfy the following constituent elements:

- information that may be used in the course of production, sales or operations;
- having the nature of secrecy;
- economic value; and
- adoption of reasonable protection measures.

To keep the trade secrets confidential during court proceedings, the court trial may be held in private if the court deems it appropriate or it is otherwise agreed upon by the parties. The parties and a third party may also apply to the court for issuing a 'confidentiality preservation order', and the person subject to this confidentiality preservation order should not use the trade secrets for purposes other than those related to the court trial or disclose the trade secrets to those who are not subject to the order.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

The Trademark Act in Taiwan provides for the protection of brands. The rights of trademarks can be obtained through registration with Taiwan's Intellectual Property Office. The term of protection is 10 years from the date of publication of the registration and may be renewed for another 10 years by filing a renewal application.

Every registered trademark will be published on the official website maintained by the Intellectual Property Office and the trademark search system is accessible to the general public. On the search system, a fintech business may check whether an identical or similar trademark exists and who the proprietor of a registered trademark is.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

Patent

With regard to infringement of an invention patent, the patentee may claim for damage suffered because of the infringement. The amount of damages may be calculated by:

- the damage suffered and the loss of profits as a result of the infringement;
- profit earned by the infringer as a result of patent infringement; or
- the amount calculated on the basis of reasonable royalties.

If the infringement is found to be caused by the infringer's wilful act of misconduct, the court may at most triple the damages to be awarded. Patent infringements have been decriminalised since 2003.

Copyright

The damage suffered because of copyright infringement may be claimed in the process of civil procedure. As for criminal liabilities, there are different levels depending on different types of infringement, ranging from imprisonment, of no more than three years, and detention to a fine of no more than NT$750,000.

Trademark

The damage suffered because of trademark infringement may be claimed in the process of civil procedure. As for criminal liabilities, any person shall be liable to imprisonment for a period not exceeding three years or a fine not exceeding NT$200,000, or both, if he or she:

- uses a trademark that is identical to the registered trademark in relation to identical goods or services;
- uses a trademark that is identical to the registered trademark in relation to similar goods or services and hence there exists a likelihood of confusion for relevant consumers; or
- uses a trademark that is similar to the registered trademark in relation to identical or similar goods or services and there exists a likelihood of confusion for relevant consumers.

On 4 May 2022, the Legislative Yuan amended the Trademark Act to stipulate that any person who intends to use identical merchandise or services with a registered trademark and a collective trademark for himself or herself or any person, and sells, manufactures, possesses, displays, exports or imports labels, tags, containers or products related to services with a sign identical or similar to another person's registered trademark or collective trademark shall be liable to imprisonment for a period not exceeding a year or a fine not exceeding NT$50,000. The same liability also applies to any person who infringes a trademark on social media and the internet. The Executive Yuan has yet to determine the effective date of this amendment.

Trade secrets

The damage suffered because of infringement of trade secrets may be claimed in the process of civil procedure. As for criminal liabilities, a person may be sentenced to a maximum of five years imprisonment and, in addition, a fine between NT$1 million and NT$10 million if he or she:

1 acquires a trade secret by an act of theft, embezzlement, fraud, threat, unauthorised reproduction or other wrongful means, or uses or discloses a trade secret that has been acquired;
2 carries out an unauthorised reproduction of, or uses or discloses, a trade secret that he or she has knowledge or possession of;
3 fails to delete or destroy a trade secret in his or her possession as the trade secret holder orders, or disguises it; or

Read this article on Lexology

4 knowingly acquires, uses or discloses a trade secret known or possessed by others that is under the circumstances specified in points (1) to (3) above.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

In April 2016, the Financial Supervisory Commission (FSC) issued a press release pointing out the regulatory issues that may arise from peer-to-peer lending activities. According to this and other sources, the FSC is of the view that:

- if it is arranged that the lender (as a member of the platform) splits the original credit into several parts and in turn allocates and 'sells' the divided parts to other 'members' for investment with high return, it might involve regulatory issues regarding multilevel marketing; or
- if the platform operators claim that the transaction has the nature of high return, low cost and low risk, it might constitute false or misleading advertising and would result in a violation of the Fair Trade Act.

The above two issues are under the supervision of the Fair Trade Commission.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

Currently, there are no tax incentives specifically provided for fintech companies.

Generally, a company may choose to credit either up to 15 per cent of its total expenditure on research and development against its corporate income tax payable for that year; or up to 10 per cent of its total expenditure on research and development against its corporate income tax payable for each of the three years starting from that year, provided that the deduction amount did not exceed 30 per cent of the corporate income tax payable for the company in that year and that it did not commit any material violation of any law on environmental protection, labour or food safety and sanitation in the past three years. To apply such tax credits, a company must apply to and receive approval from the government.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

Currently, there are no such new tax laws or guidance and, to our understanding, currently, there are no such proposals.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

The Act for the Recruitment and Employment of Foreign Professionals, as enacted in 2017, aims to attract foreign talents to increase Taiwan's competitiveness. Although this Act was not specifically enacted for the area of fintech, we believe that fintech talents would be among those that Taiwan wants to attract. The key measures proposed under this Act are:

- the relaxation of regulations on work, visa and residence;
- the easing of provisions concerning the stay or residence of parents, spouses and children; and
- providing benefits regarding retirement, insurance and tax.

In response to the demand for talent for globalisation of financial markets and the rapid development of emerging technologies, the Financial Supervisory Commission issued an amendment to 'Qualifications and Recognition of Specified Foreign Professionals with Special Expertise in the Financial Field' on 15 December 2020. The main amendments were made to relax certain minimum requirements of the period of employment for applicants with relevant qualifications.

UPDATE AND TRENDS

Current developments

41 Are there any other current developments or emerging trends to note?

New applications of cryptocurrency and blockchain technology, such as decentralised finance (DeFi) and non-fungible tokens (NFTs), have been a hot topic in Taiwan over the past one to two years.

Although the government does not seem to have given an official view or caution on the rise of DeFi activities, from a local perspective, the classification of any DeFi activities should be determined case by case, and there are currently no specific laws or regulations promulgated by the government to regulate or provide a legal basis for the development of DeFi.

Read this article on Lexology

Laws such as those relating to banking, trusts and futures would need to be reviewed to ensure legal compliance.

In December 2021, in response to the digital transformation of the insurance industry and the need to develop and promote relevant innovative insurance products, the Financial Supervisory Commission (FSC) proposed a new policy on the establishment of digital-only insurance companies, including a policy roadmap and a tentative timeline. Relevant amendments were made by the FSC for setting forth the requirements for establishing digital-only insurance companies and the relevant regulations for insurance solicitation, underwriting and claims settlement. According to the FSC's newsletter, two applications were filed with the FSC by 31 October 2022 while both of them were not approved by the FSC. According to relevant news reports, the FSC is still exploring the feasibility of re-opening for the applications of digital-only insurance companies by the end of 2023 depending on factors such as the market trend of the insurance industry.

理律法律事務所
LEE AND LI
SINCE 1965 ATTORNEYS-AT-LAW

Abe T S Sung abesung@leeandli.com
Eddie Hsiung eddiehsiung@leeandli.com

8th Floor No 555 Sec 4, Zhongxiao East Road, Taipei 11072, Taiwan
Tel: +886 2 2763 8000
www.leeandli.com

Read more from this firm on Lexology

Read this article on Lexology

Turkey

Cigdem Ayozger Ongun and Deniz Erkan
SRP Legal

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 599
General innovation climate 599
Government and regulatory support 600

FINANCIAL REGULATION 602
Regulatory bodies 602
Regulated activities 603
Consumer lending 603
Secondary market loan trading 604
Collective investment schemes 604
Alternative investment funds 605
Peer-to-peer and marketplace lending 606
Crowdfunding 607
Invoice trading 608
Payment services 608
Open banking 608
Robo-advice 610
Insurance products 610
Credit references 611

CROSS-BORDER REGULATION 612
Passporting 612
Requirement for a local presence 612

SALES AND MARKETING 612
Restrictions 612

CRYPTOASSETS AND TOKENS 613
Distributed ledger technology 613
Cryptoassets 613
Token issuance 614

ARTIFICIAL INTELLIGENCE 614
Artificial intelligence 614

CHANGE OF CONTROL 615
Notification and consent 615

Read this article on Lexology

FINANCIAL CRIME 616
Anti-bribery and anti-money laundering procedures 616
Guidance 616

DATA PROTECTION AND CYBERSECURITY 617
Data protection 617
Cybersecurity 618

OUTSOURCING AND CLOUD COMPUTING 619
Outsourcing 619
Cloud computing 620

INTELLECTUAL PROPERTY RIGHTS 621
IP protection for software 621
IP developed by employees and contractors 622
Joint ownership 622
Trade secrets 623
Branding 624
Remedies for infringement of IP 624

COMPETITION 624
Sector-specific issues 624

TAX 625
Incentives 625
Increased tax burden 626

IMMIGRATION 626
Sector-specific schemes 626

UPDATE AND TRENDS 627
Current developments 627

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

There is an ever-evolving fintech climate in Turkey. According to the Turkey Fintech Guide 2023 published by The Presidency of the Republic of Turkey Finance Office, Turkey has received a start-up investment of US$1.6 billion in 2022. According to the Guide, Turkey ranks 10th in Europe and 3rd in the Middle East and North Africa. Pursuant to the Guide, total of US$1.6 billion was invested in 300 start-ups, out of which the fintech industry received the highest number of investments with 34 deals. As a result of these 34 deals, US$90 million was invested in fintech companies in 2022, making it the year in which the highest investment amount was reached.

As of February 2023, 739 fintechs are established in Turkey, 637 of which are active. These fintech companies consist of 255 organisations that work on decentralised finance, banking technologies, and corporate finance. Also, there are 90.6 million active retail digital banking

Read this article on Lexology

users and 2 million point-of-sale terminals, 52,100 automated teller machines, 99.3 million credit cards and 71.6 million prepaid cards in Turkey. Moreover, the contactless payment rate reached 66 per cent, 18 per cent above the previous year's rate.

In the Turkish fintech ecosystem, services such as payment and e-money services, money transfer and remittance, bill payment, digital wallet and system operator services are regulated, while some issues such as lending and credit scoring are yet to be regulated. However, in less than a year, new regulations regarding open banking, service-model banking, equity and lending-based crowdfunding entered into force. With the Economic Reforms Action Plan published by the Ministry of Treasury and Finance on 12 March 2021, certain legal regulations in this area were implemented in 2021 as well as 2022.

With new developments in the regulatory area, 100 fintechs were licensed as of 2022:

- 45 e-money institutions;
- 29 payment institutions;
- eight crowdfunding platforms;
- five insurtechs;
- five payment systems;
- four digital banks;
- three financing institutions; and
- one intermediary institution.

Thirty-four fintechs received an investment of US$89 million as of February 2023, following an upward trend in fintech investments in Turkey despite the decreased global risk appetite following the covid-19 pandemic.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Different public authorities such as the Republic of Türkiye Ministry of Trade, the Republic of Türkiye Ministry of Industry and Technology, the Scientific and Technological Research Council of Türkiye (TÜBİTAK) and the Small and Medium Enterprises Development Organisation (KOSGEB) have different incentives and support schemes for financial innovation. These supports and incentives are spread over many different areas such as commission support, market entry support, strategic business plan support, software, mobile application and digital game development support.

The support is provided to entities that meet specific criteria brought by different legislations. In Turkey, investments have been supported pursuant to the Decision on State Aid in Investments brought into force with Decision of the Council of Ministers No. 2012/3305, and its Implementing Communiqué No. 2012/1. The Decision on Providing Project Based State Aid to Investments was brought into force with Decision of the Council of Ministers No. 2016/9495 and Communiqué No. 30892 on the Code of Practice of Technology-Oriented Industrial Movements Program (Communiqué No. 30892). The latest developments concern Communiqué No. 30892, which was amended with Official Gazette No. 30969.

Read this article on Lexology

Investment incentives are provided to all entities that meet the requirements pursuant to the above-mentioned laws and regulations. Unlike many information technology or e-commerce projects, fintech projects are more likely to benefit from these incentives because of the nature of fintech and its requirements such as security, payment infrastructure, user experience and mobility.

During the establishment phase of fintech start-ups, there are alternatives such as private incubation centres, techno centres and collaboration offices that may allow fintech start-ups to benefit from tax advantages. In addition to these investment incentive-focused regulations, fintech start-ups may also benefit from Technology Development Law No. 4691 and its implementing regulation. This law provides lower corporate income tax, withholding tax, income tax exemptions, employer social security contribution support payments and value added tax exemptions for fintech start-ups.

Government support is also stipulated in the 11th Development Plan of Turkey. The 11th Plan covers the year 2023 and includes objectives on fintechs. This plan commits to supporting the creation of a secure financial technology ecosystem that provides equal opportunities for firms by drawing on international best practices.

To bring this goal to life, it is aimed to create a roadmap which will be for the development of the fintech ecosystem in Turkey and the coordination of implementation will be ensured by a single public institution. On top of that, to strengthen the legal infrastructure of open banking, it is aimed to achieve legislative harmonisation with EU Directive (EU) 2015/2366 (Payment Services Directive II) (PSD2), to establish the Istanbul Finance and Technology Base, to establish the Regulatory Experimental Area and Industry Experimental Area and to establish the Association of Payment Services and Electronic Money Institutions.

According to the amendment to Presidential Decree No. 2834, published in Official Gazette No. 31207 of 8 August 2020; as of 23 March 2022, the rate of Bank and Insurance Transactions Tax is applied as:

- 1 per cent on the proceeds received in return for the acquisition or disposal of domestic Turkish lira-denominated bonds with repurchase and resale commitment;
- 1 per cent on the proceeds received in return for the sale of domestic Turkish lira-denominated bonds without waiting for maturity;
- 10 per cent on the proceeds received in return for consumer loans; and
- 5 per cent on the proceeds received in return for other bank and insurance transactions.

The Amendment to the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions (the Amendment), in line with the requirements of PSD2, entered into force on 1 January 2020. The Amendment set forth a provision for the establishment of the Turkish Payment Services and Electronic Money Association (the Association), which entered into force on 22 May 2020. Accordingly, all payment and electronic money institutions are required to become members of the Association.

The Strategy and Budget Directorate of the Presidency of the Republic of Turkey published the Presidential Annual Program for 2023. The establishment of a secure fintech ecosystem that provides equal opportunities for companies as well as the establishment of interfaces and standards that will strengthen cooperation and information sharing for the digital

transformation of the manufacturing industry are within the scope of the Presidential Annual Program.

Finally, Presidential Circular No. 2022/10 published in the Official Gazette of 10 June 2022, identifies subjects such as development of financial services, entrepreneurship and small and medium-sized enterprises, as well as information and communication technologies as issues to be worked on in the 12th development plan.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

Regulatory and supervisory bodies include the Ministry of Treasury and Finance, the Central Bank of the Republic of Turkey (CBRT), the Banking Regulation and Supervision Agency, the Capital Markets Board, and the Insurance and Private Pension Regulation and Supervision Agency. These institutions carry out their duties in different parts of the fintech sector.

The CBRT is authorised in regulating payment systems, electronic money institutions and payment institutions. The CBRT is entitled to issue payments, e-money and system operator licences pursuant to Law No. 6493, the Regulation on Payment Services and Electronic Money Issuance and Payment Institutions.

In addition to the CBRT, the Turkish Financial Crimes Investigation Board (MASAK), which acts as Turkey's financial intelligence unit, effectively fights money laundering and terrorist financing (anti-money laundering (AML)). MASAK checks whether financial institutions meet the requirements of AML regulations and laws. Therefore, fintech companies, such as payment service providers, cryptocurrency trading platforms and crowdfunding platforms, must fulfil their AML obligations.

The sale and marketing of financial services and products may fall under the supervision of the Turkish Capital Markets Board (CMB) or the Banking Regulation and Supervision Agency (BRSA). The CMB's Communique on Principles on Investment Services and Activities and Ancillary Services No. III-37.1 and the BRSA's Regulation on Bank's Procurement of Support Services impose certain restrictions on financial service providers as well as the vendors providing the sales and marketing of financial services in Turkey. Therefore, the BRSA is authorised regarding digital banking, service model banking and financing companies.

Article 6 of the Regulation on Establishment and Activities of Asset Management Companies sets forth that asset management companies must obtain authorisation from the CMB prior to their establishment to carry out their activities. According to the Banking Law and the Financial Leasing Law, only entities with a licence granted by the BRSA may legally conduct lending activities. However, following the entry into force of the Amending Law, new licences have been granted by the CBRT as of 1 January 2021.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Payment systems, electronic money institutions and payment institutions require licencing in Turkey. As for financial activities, a large amount of financial services trigger licensing, authorisation or registration in Turkey. These activities might be regulated by the CBRT, the CMB, the BRSA, the Ministry of Treasury and Finance or the Central Securities Depository of the Turkish Capital Markets.

The CBRT authorises services such as invoicing services, e-money services and system operator services while the BRSA issues licences for banking and finance activities such as banking services, factoring and financial leasing services. The Capital Market Authority, on the other hand, is responsible for authorising equity and lending-based crowdfunding platform services, trading and carrying out intermediation activities in securities and other capital markets instruments. The Ministry of Treasury and Finance authorises insurance activities and the Central Securities Depository of the Turkish Capital Markets provides its members with registration (public offering, etc), settlement and custody services.

In addition to these regulatory bodies, the Risk Centre established within the Banks Association of Turkey collects risk data and information of clients of credit institutions and other financial institutions to be deemed eligible by the Banking Regulatory and Supervisory Board, ensuring that such information is shared with said institutions or with the relevant persons or entities themselves, or with real persons and private law legal entities if approved or consented; and Kredi Kayıt Bürosu (KKB) conducts all operational and technical activities through its own organisation as an agency of the Risk Center of the Banks Association of Turkey and provides data collection and sharing services.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Consumer lending is regulated within the scope of the Banking Law, the Law on Bank Cards and Credit Cards, the Regulation on Credit Operations of Banks and by the Ministry of Commerce through the Consumer Law, the Regulation on Consumer Loan Agreements and the Regulation on Housing Finance Agreements.

With the Decision No. 10222 taken on 9 June 2022 by the Banking Regulation and Supervision Board, the following rates regarding consumer loans were announced:

- the general maturity limit for consumer loans shall be set as 24 months for loans with a loan amount above 50,000 Turkish liras and below 1,000 Turkish liras and 12 months for loans with a loan amount above 100,000 Turkish liras; and
- the minimum payment amount for credit cards with a limit below 25,000 Turkish liras shall be set as 20 per cent of the period debt, and the minimum payment amount for credit cards with a limit above 25,000 Turkish liras shall be set as 40 per cent of the period debt.

In addition, Decision No. 10222 stated that the necessary steps would be taken in the following areas:

- differentiation of the loan-to-value ratio in housing loans on an amount basis;
- directing loans to productive areas such as investment and exports to improve the selective approach, particularly for commercial loans;
- increasing the risk weight of loans to be extended to legal entities that engage in derivatives transactions with non-residents; and
- introducing the possibility of allocated swaps for non-residents.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

In Turkey, in principle, loans can only be provided by banks and credit institutions that do not include payment services or e-money institutions. The prohibition on lending is specifically regulated in the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers. Within the scope of this Regulation, payment and e-money institutions cannot give loans, nor may they engage in advertising and marketing activities in a way that creates the impression that they are giving loans. Additionally, loan-based transactions are subject to the Turkish Banking Law and regulations. Transferring a loan by way of novation (namely, discharging the original debt) will have the effect of extinguishing the Turkish law-governed security. In these cases, there is a requirement to re-establish the security for the new lender. A parallel debt structure may be a way of preventing the fall of the accessory security as a result of novation. The transfer of debts is also possible and made by an agreement between the transferor, the transferee and the debtor. Security providers for these debts should provide their consent in written form. There are no registration requirements with the authorities in Turkey for a transfer or assignment to be effective.

On the other hand, debt instruments, which can only be provided by the above-mentioned institutions, can be purchased and sold in the secondary market under the Capital Markets Law and regulations. Borsa İstanbul AŞ (BIST) is the most active and organised Developer Interest Bearing Scheme secondary market in Turkey. The bonds and bills markets are outright purchase and sales and repo and reverse-repo markets. Intermediary institutions and banks can participate in these markets, and the rules of BIST are valid. In BIST, of which the CBRT is also a member, participants send their requests and proposals to the BIST system with all the necessary details. When the best demand and offer are met in the system, transactions are carried out within the framework of the determined operating rules.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

In Turkey, the general rules and principles regarding investment funds are regulated under the Capital Markets Law and regulations. In this respect, further details regarding the

establishment and activities of investment funds are regulated under the Communiqué on the Principles of Investment Funds (III-52.1). Accordingly, the Investment Funds Guide clarifies the rules and principles stipulated in this Communiqué.

The regulatory regime for collective investment schemes is new, and equity and lending-based crowdfunding platforms have been highly regulated under the Capital Markets Law. The Communiqué on Crowdfunding (III-35/A.2) was issued by the CMB and was published in the Official Gazette of 27 October 2021. As per this Communiqué, only the platforms authorised and listed by the CMB may carry out equity-based and lending-based crowdfunding activities.

Additionally, peer-to-peer lending is not currently regulated in a manner synonymous with the definition found under EU Directive (EU) 2015/2366 (Payment Services Directive II) (PSD2). However, debt-based crowdfunding platforms, which can be considered peer-to-peer lending, have been regulated. Regarding the platforms on which crowdfunding activities can be carried out, the Capital Markets Law and Communiqué No. III-35/A.2 on Crowdfunding can be mentioned as the first Turkish legal document that regulates lending-based crowdfunding platforms, which can be considered as peer-to-peer lending.

The Amending Law, which was published in Official Gazette No. 31050 of 25 February 2020, entering into force on the same date, introduced the concept of crowd-lending by the inclusion made to Law No. 6362. With regard to crowdfunding, with the amendment made in the first paragraph of article 35/A of Law No. 6362 and Crowdfunding Communiqué (III-35/A.2), the CMB is empowered to make determinations regarding crowdfunding activities that collect money from the public based on partnership or lending.

As per the Amending Law, the provisions of banking legislation shall not be applied for financing provided through lending-based crowdfunding and shall not be considered as deposit or participation fund acceptance. This situation brings an alternative to conventional and participation banking models, especially in financing innovative projects with industrial and technology companies. In addition, with the amendments made to article 35A of Law No. 6362, responsibility regarding the information form on the crowdfunding transactions is clarified and venture companies, whose shares are monitored and recorded, are now allowed to hold general assembly meetings electronically.

It has also been stipulated that crowdfunding platforms shall not be subject to the provisions of the Capital Markets Law regarding publicly held corporations, public offerings, issuers, the obligations of issuing prospectuses and issuance documents, investment services and activities, ancillary services and exchanges, market operators and other organised marketplaces.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

Alternative investment funds (AIFs) are operated and managed by portfolio management companies on behalf of their investors in exchange for a consideration, namely, a participation share. Managers of AIFs are subject to the Communiqué on Portfolio Management Companies and Activities of Such Companies (III-55.1) issued by the Capital Markets Board.

Read this article on Lexology

This Communiqué has been amended as per the Communiqué (III-55.1.d) (Amending Communiqué), published in the Official Gazette of 18 February 2023, which entered into force on the same date.

The Amending Communiqué introduced the concept of 'sub-portfolio management', which includes a contract to be signed between institutions or asset management companies authorised for portfolio management abroad for sub-portfolio management. Within the framework of this agreement, it refers to the activity of managing a certain portion or all of the portfolio of the portfolio manager by the sub-portfolio manager.

In addition, portfolio management companies are required to be established as joint-stock companies with the main objective of operating and managing investment funds. Compliance with certain conditions and obtaining the CMB licence as set forth under the above Communiqué are required for establishing and operating a portfolio management company (PMC). The manager can either be the founder (founding a PMC or real estate PMC (REPMC)) or hold another role in the PMC or REPMC pursuant to a portfolio management contract. Fintech companies do not fall under the scope of the legislation concerning alternative investment fund managers.

With the Amending Communiqué, the minimum paid-in capital amount required for a portfolio management company's establishment permit to be evaluated by the CMB has been increased from 6 million Turkish liras to 30 million Turkish liras. Also portfolio management companies, in addition to opening branches and establishing agencies with banks and brokerage houses, are now able to open liaison offices in Turkey or abroad with the permission of the CMB.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Lending activities are highly regulated by the BRSA. For instance, according to the Banking Law or the Financial Leasing Law, only the entities with a licence granted by the BRSA can legally conduct lending activities. According to Turkish Criminal Code No. 5237, money lending and earning interest from that money without holding a licence is a crime, defined as usury, that is subject to imprisonment between two to six years and a monetary fine from 500 days to 5,000 days. In addition, peer-to-peer lending is not currently regulated in a manner synonymous with the definition found under PSD2.

The Capital Markets Law and Communiqué No. III-35/A.2 on Crowdfunding regulate the lending-based crowdfunding platforms, which can be considered peer-to-peer lending. This Communiqué divides crowdfunding activities into two categories:

- equity-based crowdfunding; and
- debt-based crowdfunding.

Debt-based crowdfunding activities are defined as fund-raising from the public through platforms in return for crowdfunding debt securities and equity-based crowdfunding on the

other hand is defined as fund-raising from the public through crowdfunding platforms in return for shares.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

Equity and debt-based crowdfunding platforms are highly regulated under the Capital Markets Law (CML). Communiqué No. III-35/A.2 on Crowdfunding entered into force upon its publication in the Official Gazette of 27 October 2021 and designates the CMB as the supervisory regulatory authority. The Communiqué repealed the Communiqué on Equity Based Crowdfunding (No. III-35/A.1), and lending and share-based crowdfunding are now regulated in a single communiqué.

Equity crowdfunding platforms are defined as platforms that allow entrepreneurs or companies to raise the funds they need for a project or venture idea electronically. Project owners or entrepreneurs and investors through platforms that allow investment in return for shares have come together through platforms that allow investment in return for an equity. Debt-based crowdfunding on the other hand is defined in the Communiqué as collecting money from the public through platforms in exchange for a debt instrument, and the funding process is carried out through platforms where investors who want to invest and entrepreneurs and companies seeking funds come together.

As per the Communiqué, crowdfunding activities shall be conducted via crowdfunding platforms, which can be joint-stock companies solely providing crowdfunding services; or investment institutions that are development and investment banks, participation banks or intermediary institutions.

With the Communiqué as a general rule, platforms will be able to solely carry out share-based and (or) debt-based crowdfunding activities; however, development and investment banks, participation banks and intermediary institutions are exempt from this rule. The principles to be followed while conducting crowdfunding activities will be set out in a written crowdfunding agreement to be executed between the fundraisers and the platform. In addition, the Communiqué paves the way for small or medium-sized technology and production companies to raise funds from capital markets without publicly offering shares.

With this being said, not all types of crowdfunding platforms are regulated in Turkish legislation. For example, reward-based crowdfunding platform activities are not regulated in Turkey while donation-based crowdfunding platforms are and may be subject to certain regulations. Even though there is no specific regulation regarding reward-based crowdfunding platforms, both reward- and donation-based crowdfunding platform activities have been performed by several companies in Turkey.

Finally, crowdfunding activities are not characterised as investment services or ancillary services in the CML. The reason for excluding crowdfunding transactions from the scope of investment and ancillary services is that crowdfunding activities are regulated to prevent small-scale companies from having cash difficulties, and therefore, general provisions are applied to the relationship between the parties. However, to make it easier for entrepreneurs

to raise funds, crowdfunding platforms are not included in the scope of investment institutions operating under limited conditions and a flexible approach is followed.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

The accounts receivable are usually, but not always, in the form of cheques or cashier's cheques assigned or transferred to the assignee by the assignor in return for immediate payment. The Law on Financial Leasing, Factoring and Financing Companies and its secondary regulations are the primary pieces of legislation that govern this field in Turkey.

In addition, establishing a platform to provide information and services regarding electronic invoices to merchants, is not regulated in Turkish jurisdiction. However, providing services for mediating invoice payments is subject to Law No. 6493.

Payment services

12 | Are payment services regulated in your jurisdiction?

Payment services are regulated in Turkey under Law No. 6493. According to Law No. 6493, the following activities are defined as payment services:

- all the operations required for operating a payment account, including the services enabling cash to be placed on a payment account and cash withdrawals from a payment account;
- payment transactions, including transfers of funds from the payment account of a payment service user before the payment service provider; direct debits, including one-off direct debits, execution of payment transactions through a payment card or a similar device, and the execution of money transfers, including regular standing orders;
- issuing or acquiring payment instruments;
- money remittance;
- executing payment transaction where the consent of the payer to execute a payment transaction is given by means of any information technology or electronic telecommunication device and the payment is made to the information technology or electronic telecommunication operator, acting only as an intermediary between the payment service user and the supplier of the goods and services; and
- services for mediating invoice payments.

Open banking

13 | Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

The term 'open banking' was defined for the first time in the Banks' Information Systems and Electronic Banking Services (the Regulation) published in the Official Gazette of 15 March 2020, and came into force on 1 January 2021. Pursuant to the Regulation, remote identification and digital onboarding have been regulated for the first time. In this context,

open banking services may now be used for digital identity. Electronic money and payment institutions are required to comply with the Regulation by 30 June 2023.

Additionally, the Regulation on the Operating Principles of Digital Banks and Service Model Banking has been published in Official Gazette No. 31704 of 29 December 2021. Within the scope of the Regulation, digital banks are provided with the opportunity to perform all the activities that credit institutions can perform, depending on whether they are deposit or participation banks, unless otherwise stated in this Regulation or related sub-regulations. Also, with the Regulation on Operating Principles of Digital Banks and Service Model Banking, the principles of service model banking have been regulated, and service banks will be able to provide service model banking services only to domestically resident interface providers and only within the framework of their own operating permits.

Most importantly, with the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers, the payment service providers are now obliged to offer the payment account and infrastructure services it offers under similar conditions with other commercial customers, business partners and other payment service providers with which it makes transactions, if another payment service provider wishes to use said services and within one month at the latest, the payment service provider is obliged to convey the decision of rejection or acceptance to the requesting payment service provider.

Also, with Law No. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, the CBRT is authorised to determine all procedures and principles regarding the service of presenting consolidated information regarding one or more payment accounts of the payment service user with payment service providers on online platforms, provided that the payment service user's approval is obtained and the payment order initiation service for the payment account in another payment service provider at the request of the payment service user.

With the Communiqué on Information Systems of Payment and Electronic Money Institutions and Data Sharing Services in the Field of Payment Services of Payment Service Providers, which was published in the Official Gazette of 1 December 2021, the procedures and principles regarding the electronic channel through which the parties acting on behalf of the customers can remotely access the payment services offered by the account service providers via APIs and perform the transactions within the scope of the law or instruct the account service providers to carry out such transactions were regulated.

In addition, the Banking Sector Good Practices Guide on the Protection of Personal Data (Guide) was published by the Personal Data Protection Authority on 5 August 2022, specifically mentioning the open banking systems. The Guide contains general explanations regarding the procedures and principles that banks must comply with in the field of personal data protection and the obligations to be fulfilled. Regarding open banking, the Guidelines mention that there are three main processing activities in open banking services:

- processing of personal data of the natural person customer by the bank for the purpose of providing banking services;
- processing of personal data of the natural person customer by a third-party provider for the purpose of enabling the natural person customer to benefit from open banking products and services; and

Read this article on Lexology

- transfer of certain categories of personal data of the natural person customer by the bank to the third-party provider and simultaneously the third-party provider records these data in its own data recording system.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

In Turkey, there is no legal regulation specifically regarding robo-advisory or automatic consultancy. For this reason, there is no automated consultancy company that serves in an open architectural structure, can provide investment consultancy services to its customers and can act on their behalf. The institutions that are allowed to conduct consultancy activities regarding fund allocation and to provide fund advice to the participant are portfolio management companies subject to the Capital Markets Law.

Even though automatic consultancy services are not directly available to the participant, currently, Turkish automatic consultancy products are used by companies such as pension companies. However, the Digital Transformation Office, structured under the Presidency, is granted the task of leading the artificial intelligence (AI) transformation process.

In this context, the National Artificial Intelligence Strategy 2021–2025, drafted in cooperation with the Digital Transformation Office of the Presidency of the Republic of Turkey and the Ministry of Industry and Technology, was announced on 24 August 2021, and the Presidential Circular on the National Artificial Intelligence Strategy was published in the Official Gazette of 20 August 2021. In this respect, the National Artificial Intelligence Strategy Steering Committee was established under the chairmanship of the Vice President with the participation of the President of the Digital Transformation Office and the relevant Deputy Minister of the Ministry of Industry and Technology, to further the activities that Turkey will carry out in the field of AI until 2025, to determine the strategic priorities, goals, targets and measures in this field and to implement them.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Insurance services and, accordingly, selling insurance products are highly regulated under the Turkish Insurance Law and regulations. Companies that decide to perform these activities must obtain authorisation from the Ministry of Treasury. As the activities of insurance companies are restricted, they are not allowed to perform activities other than providing insurance services. In this respect, fintech companies must pay attention not to be considered insurance companies by facilitating activities in the insurance market.

Additionally, the Regulation on Collecting, Storing and Sharing Insurance Data, prepared by the Insurance and Private Pension Regulation and Supervision Authority (Authority) within the scope of Insurance Law No. 5684 (Regulation), has been published in the Official Gazette

and entered into force on 18 October 2022. The regulation determines the scope, procedures, and principles regarding the processing, sharing, and transfer of insurance data.

Pursuant to the Regulation the Authority is vested with the authority to determine the following:

- procedures and principles regarding processing activities regarding insurance data such as obtaining, storing and using insurance data from private legal entities, public institutions and organisations, public professional organisations and their superior organisations and information centres; and
- procedures and principles regarding the transfer of these data to insurance companies, reinsurance companies and pension companies engaged in insurance activities.

Pursuant to the Regulation, insurance data shall be collected by the Insurance Information and Monitoring Center from entities such as private legal entities, public institutions and organisations, and public professional organisations and must be kept in a general database.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

The Credit Registration Bureau (Kredi Kayıt Bürosu (KKB)) offers its services not only to financial institutions, but also to individuals and the real sector through the cheque report, risk report and electronic report systems launched in January 2013. Since September 2014, KKB gathered its services aimed at individuals and the real sector under the umbrella of Findeks, the consumer service platform of KKB.

Providing credit references or credit information services in Turkey is a regulated activity under Law No. 5411. The Risk Center was established within the Banks Association of Turkey (TBB) to collect the risk data and information of clients of credit institutions and other financial institutions to be deemed eligible by the Banking Regulatory and Supervisory Board and ensure that this information is shared with these institutions or with the relevant persons or entities themselves or with real persons and 61 private law legal entities if approved and consented to.

The KKB was founded in accordance with article 73/4 of the Banking Law and it conducts all operational and technical activities through its own organisation as an agency of the Risk Center of the TBB and provides data collection and sharing services to the 187 financial institutions that are members of the Risk Center.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

Pursuant to the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers, which was published in Official Gazette No. 31676 of 1 December 2021, fintech companies may cooperate with legal entities residing abroad when providing services. However, the legal entities residing abroad are to obtain permission from the Central Bank of the Republic of Turkey (CBRT), in line with their objectives or operations. However, the foreign legal entity in question must also be authorised to provide payment services or issue electronic money, by the relevant authorities of the country where its head-quarters is located. The legal entity residing abroad with whom the cooperation is made may not be the exposed face of the service alone before the customer and the payment institutions and e-money institutions will continue to be accountable to domestic customers for the services provided within the scope of the cooperation.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

Under Turkish law, a licence to provide financial services in Turkey cannot be obtained unless the company is governed by Turkish law; however, pursuant to the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers, it is determined that fintech companies may cooperate with institutions abroad when providing financial services. A fintech company is required to be incorporated and licensed in the local Turkish jurisdiction by the CBRT. The requirement also applies to companies that provide cross-border services and products, and whether the products are actively marketed or the client in the jurisdiction solicits the service or product, is not relevant.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

The sale and marketing of financial services and products may fall under the surveillance of the Capital Markets Board (CMB) or the Banking Regulation and Supervision Agency (BRSA). The CMB's Principles on Investment Services and Activities and Ancillary Services No. III-37.1 and the BRSA's Regulation on Banks' Procurement of Support Services impose certain restrictions on financial service providers and the vendors providing the sale and marketing of financial services in Turkey.

Besides these regulations, the prohibition on lending is specifically regulated in the Regulation on Payment Services and Electronic Money Issuance and Payment Service

Providers. Within the scope of this regulation, payment and e-money institutions cannot give loans, nor may they engage in advertising and marketing activities in a way that creates the impression that they are giving loans.

According to the BRSA press release of 15 December 2022, to avoid any doubt, it has been announced that only authorised institutions listed under the Institutions tab on the BRSA's official website are allowed to provide loans. The loans must be provided by banks and other financial institutions operating with permission from the BRSA and institutions explicitly authorised by the relevant legislation.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

There are neither rules nor regulations governing the use of distributed ledger technology or blockchains. However, distributed ledger technology and blockchains have recently started to be used in various sectors, including the banking and finance sector.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

The Regulation on Not Using Crypto Assets in Payments was published by the Central Bank of the Republic of Turkey (CBRT) in the Official Gazette of 16 April 2021, entering into force on 30 April 2021. The Regulation regulates:

- not using cryptoassets in payments;
- procedures and principles are determined to ensure that cryptoassets are not used directly or indirectly in the provision of payment services and issuance of electronic money; and
- payment and electronic money institutions do not act as intermediaries for platforms that provide trading, custody, transfer or issue services regarding cryptoassets or fund transfers from these platforms.

Payment service providers (banks, electronic money and payment institutions, Posta ve Telgraf Teşkilatı AŞ) are not allowed to develop business models in a way that cryptoassets will be used directly or indirectly in the provision of payment services and issuing electronic money. In addition, payment and electronic money institutions are prohibited from inter-mediating on platforms that provide trading, custody, transfer or issue services regarding cryptoassets or fund transfers to be made from these platforms.

The Turkish Financial Crimes Investigation Board published an updated guidebook that states that fund transfers made to intermediary institutions for the purpose of purchasing

cryptoassets (namely, bitcoin) will no longer automatically be considered a suspicious movement of funds and will be analysed on a know-your-customer basis.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

The Capital Markets Law and regulations govern the operation of digital currency exchanges and brokerages. However, cryptoassets do benefit from these rules and regulations. If an ICO project is characterised as crowdfunding, the ICO process should be carried out not by the entrepreneur, but through a crowdfunding platform.

The issue of whether there are any legal obstacles to ICO under Turkish law or whether the ICO is subject to any specific procedure varies according to the legal nature of the asset value collected from the public within the scope of the ICO organised and the features of the token to be distributed in return for this asset value. In this context, the token, which will be distributed independently of the legal nature of the asset value to be collected from the public as a fund, can be qualified as a capital market instrument due to the features it contains, and this may require adding capital market regulations to the ICO equation to be organised.

Last, pursuant to the Regulation on the Non-Use of Crypto Assets in Payments, published in the Official Gazette of 30 April 2021, no ban was imposed on the trading of cryptocurrencies on exchange platforms.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

There are neither rules nor regulations governing the use of artificial intelligence (AI) in Turkey. However, the Digital Transformation Office, structured under the Presidency, has been granted the task of leading the AI transformation process. In this context, the National Artificial Intelligence Strategy 2021–2025, drafted in cooperation with the Digital Transformation Office of the Presidency of the Republic of Turkey and the Ministry of Industry and Technology, was announced on 24 August 2021, and the Presidential Circular on the National Artificial Intelligence Strategy was published in the Official Gazette of 20 August 2021. The roadmap for work in the field of AI until 2025 has been determined by the Strategy Document. In this direction, the National Artificial Intelligence Strategy Steering Committee has been established to further the activities that Turkey will carry out in the field of AI until 2025, to determine the strategic priorities, goals, targets and measures in this field and to implement them.

The Personal Data Protection Authority published the guide titled 'Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence' on 15 September 2021. The Guide states the general recommendations set certain recommendations on the protection of personal data in AI applications, carried out by developers, manufacturers, service providers and decision-makers in the field of AI. The Guide recommends that special attention be paid to:

- personal data privacy in a way that is consistent with national and international regulations;
- relevant academic institutions, experts and organisations should collaborate within the design phase of human-rights-based ethical and socially oriented AI applications;
- the data subjects should be given the right to object to personal data processing activities that are based on technologies that affect their opinions and personal development;
- alternatives that have less interference with personal rights should be provided to ensure the freedom of choice of users; and
- mechanisms should be designed to inform the data subjects and obtain approval in necessary situations in accordance with Turkish Personal Data Protection legislation.

In addition, the Regulation on the Structure and Activities of the Türkiye Health Data Research and Artificial Intelligence Applications Institution was published in the Official Gazette of 12 March 2022. With the Regulation, the establishment, structure, duties, authorities, working principles and procedures of the Türkiye Health Data Research and Artificial Intelligence Applications Institute is regulated. This Regulation aims to increase the use of health data and AI in Turkey as well as conduct supporting scientific and technological research in this context; to provide financial or scientific support and coordinate and monitor research and development activities to be carried out on the use of AI and health data.

The Regulation on Remote Identification Methods to be used by Leasing, Factoring, Financing and Savings Financing Companies and the Establishment of Contractual Relationships through Electronic Media has been published in the Official Gazette of 11 January 2022. The Regulation includes a provision regulating to the AI applications in the sector. According to article 14 of the Regulation, the Banking Regulation and Supervision Agency is authorised to determine the implementation principles for transactions not exceeding 7,500 Turkish liras and carried out by means of AI-based methods instead of a client representative.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Pursuant to Communiqué No. 2022/2, published in the Official Gazette of 4 March 2022, the Competition Authority (Authority) made critical amendments to Communiqué No. 2010/4 on Mergers and Acquisitions Requiring Authorisation from the Competition Board in terms of the undertakings subject to the Communiqué, turnover thresholds and additional notification obligation.

Read this article on Lexology

In addition to this, some companies performing in the banking and finance sector, such as payment service providers, crowdfunding platforms, banks and financial institutions, that are supposed to be parties to business transactions (namely, mergers, acquisitions or share transfers) must notify the relevant authorities (namely, the Banking Regulation and Supervision Agency, the Central Bank of the Republic of Turkey and the Capital Market Authority).

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Turkish money laundering and terrorist financing legislation, namely, the Law for Preventing Laundered Criminal Income (Law No. 5549) and its supplementary regulation, requires that fintech companies implement procedures to combat bribery. The appointment of a compliance officer, identity verification of account holders and reporting of suspicious transactions are commonplace requirements the regulation imposes on fintech companies. The Turkish Financial Crimes Investigation Board (MASAK) also regulates fintech products and services in terms of money laundering proceedings for crime and terrorist financing.

Additionally, the term 'financial group' has been defined in article 2 of the Law on the Prevention of Laundering Proceeds of Crime with the amendment made pursuant to article 20 of Law No. 7262 on Preventing Financing of Proliferation of Weapons of Mass Destruction (Law No. 7262), of 27 December 2020. The term has been defined as to also include foreign-based financial companies.

The Regulation Amending the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism (Decision No. 6702) (Amending Regulation) has been published in the Official Gazette of 14 January 2023.

As per the Amending Regulation, the limit for certain institutions such as banks, institutions other than banks authorised to issue debit cards or credit cards, financing and factoring companies and financial leasing companies, namely obligors, to determine the identity of their customers and those acting on behalf of or on account of their customers and to take necessary measures to reveal the real beneficiary of the transaction by obtaining information on identity and confirming the accuracy of this information in cases where the transaction amount or the total amount of more than one interconnected transaction has been raised to185,000 Turkish liras or more.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

Yes, both industry and regulatory authorities provide assistance to entities active in regulated industries. MASAK, mandated by the Ministry of Treasury and Finance, provides

guidance and education. MASAK has issued Sectoral Guidance Notes addressing Financial Institutions and Banks but not specifically addressing the fintech companies.

MASAK's Guide, published on 4 May 2021, first provides brief explanations regarding the activities of MASAK and the crimes of laundering proceeds of crime and financing of terrorism. As for the definition of 'cryptoasset', the Guide refers to the Regulation Prohibiting Payments Through Crypto Assets, which was published in Official Gazette No. 31456 of 16 April 2021 and entered into force on 30 April 2021. The Guide defines the activities of cryptoasset service providers as 'the mediation regarding the trading of the cryptoassets through electronic transaction platforms'.

In addition, following the cryptoasset service providers being determined as obliged parties by the relevant legal regulation, the Suspicious Transaction Reporting Guide (Guide) was published on the official site of MASAK on 18 April 2022, aiming to explain the rules to which cryptoasset service providers are subject to regarding the obligations stipulated under Law No. 5549, including reporting of suspicious transactions.

The Guide includes explanations on the subject, form and content of the notification to be made, the types of suspicious transactions and the types of customers making the transaction. Suspicious transactions shall be notified to MASAK by the obliged parties within 10 business days at the latest from the date of suspicion regarding the transaction, or immediately in cases where there is a risk of delay. Suspicious transaction notification to MASAK in cryptoasset service providers shall be carried out by the obliged natural person him or herself or by the legal representatives of the obliged legal entity. If the obligation to report suspicious transactions is violated, the obliged party may be subject to an administrative fine of at least 50,000 Turkish liras and up to 4 million Turkish liras for each violation.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The Personal Data Protection Law, the Regulation on the Erasure, Destruction, or Anonymisation of Personal Data and the other secondary regulations are the main regulations that regulate personal data processing activities for all sector players, including fintech companies.

On the other hand, payment service providers must obtain a Payment Card Industry Data Security Standard certificate and comply with its principles and procedures, which also include rules regarding data erasure, transfer, destruction and processing. Moreover, they must keep all data in Turkey under the Communiqué on the Administration and Auditing of Payment Institutions and Electronic Money Institutions' Information Systems.

The Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers (Regulation) includes the term 'sensitive customer data' and defines it as personal data and customer security information used in issuing payment orders or verifying the

identity of the customer, and which, if captured or changed by third parties, may allow fraud or fraudulent transactions on behalf of the customer.

In this context, fintech companies are obliged to take the necessary measures for the protection of secrets and personal data, especially sensitive customer data and data belonging to themselves, in the procurement of external services.

With the Regulation, the payment service providers are obliged to offer the payment account and infrastructure services it offers under similar conditions with other commercial customers, business partners and other payment service providers with which they make transactions, if another payment service provider wishes to use such services and within one month at the latest, payment service providers are obliged to convey the decision of rejection or acceptance to the requesting payment service provider.

Also, within the scope of the Regulation, the payment services and electronic money institutions, are obliged to take the necessary measures for the protection of secrets and personal data, especially sensitive customer data belonging to itself and its customers, in the procurement of outsourcing.

The procedures and principles regarding the status of competition-sensitive data in data sharing to be made pursuant to the Regulation are determined by the Central Bank of the Republic of Turkey by taking the opinion of the Competition Authority.

Lastly, pursuant to the Communiqué on Information Systems of Payment and Electronic Money Institutions and Data Sharing Services of Payment Service Providers in the Field of Payment Services, financial institutions are obliged to inform the Personal Data Protection Authority, as soon as possible, in the event that a cyber incident that leads to the leakage or disclosure of sensitive customer data or personal data exists or personal data is illegally obtained by others.

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

Article 31 of Law No. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions levies the duty to uphold a secure information technology system on the licensed payment service provider.

Additionally, the Communiqué on the Administration and Auditing of Payment Institutions and Electronic Money Institutions' Information Systems sets clear regulatory standards applicable to fintech businesses. The Communiqué on Principles Applicable to Banking Information Systems Management published by the Banking Regulation and Supervision Agency also regulates the field of cybersecurity applicable to financial institutions, however, it does not govern payment service providers and e-money institutions.

Pursuant to the Communiqué, payment and electronic money institutions are obliged to carry out cyber security incident and breach management within the framework of predetermined procedures to ensure that incidents and breaches, including customer complaints, are detected, intervened, recorded, reported in a timely manner; analysed in a manner that

includes determining the potential size, impact, damage and affected customers; resolved in the shortest possible time and with the least damage so that information system services are restored and all relevant stakeholders are informed about the incident.

Additionally, the Electronic Communications Law also governs the issue of cybersecurity pertinent to businesses active in the fintech industry, namely, with its supplemental Regulation titled Network and Information Security in the Electronic Communications Industry published in Official Gazette No. 29059 of 13 July 2014.

Finally, the Presidential Circular on Information and Communication Security Measures sets forth a series of measures aimed at increasing the security of critical data, including requirements for the domestic localisation of data and limitations on the use of cloud services. The Circular primarily concerns public institutions and organisations, but also private organisations that provide services in critical infrastructure sectors, namely banking and finance.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Outsourcing limitations exist in two areas. One is related to outsourcing where the outsourcing also needs to carry the qualifications and standards that are required from the entity (the licensed outsourcer, in other words, the payment service provider) that is being licensed. This is detailed within Law No. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions and its secondary regulations.

The second legal requirement concerns outsourcing services pertinent to personal data and transferring personal data abroad. Red tape exists for transfers abroad; practically, a de facto rule requiring all processing activities to be performed within Turkey.

Within the scope of the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers published in the Official Gazette of 1 December 2021, the rule is that payment institutions and e-money institutions may not outsource the activities regarding providing payment services and issuing electronic money. However, with the Regulation, they have the opportunity to procure information systems, marketing, advertising, corporate resource management, accounting, call centre, follow-up activities of the institution's administrative affairs, as well as activities other than payment service provision and electronic money issuance, from an external service provider.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

There are no specific requirements focused on the use of cloud computing. However, depending on where the cloud data is physically located, the use of cloud computing may be restricted, forbidden or conditioned. For instance, the Personal Data Protection Law (Law No. 6698) regulates personal data transfer in two subsections concerning transfers within Turkey and transfers out of Turkey, respectively. Therefore, depending on where cloud data is physically located, the relevant requirements and conditions must be fulfilled. For instance, if there is a cross-border personal data transfer generated from the use of cloud computing, the data controller may be obliged to enter into an agreement with the cloud computing service provider and apply to the Personal Data Protection Board to get its authorisation.

According to the Communiqué on the Management and Supervision for Information Systems of the Payment Institutions and E-Money Institutions, institutions are obliged to have their information systems located in Turkey and cloud computing must be within the scope of these systems.

In addition, pursuant to the Information Systems Management Communiqué No. VII-128.9 published by the Capital Markets Board, companies, institutions and other legal entities are obliged to have their information systems located in Turkey (cloud computing is included in the scope of these systems). The legal entities listed in the Communiqué include publicly held companies, stock markets and capital markets institutions.

Also, The Regulation on the Independent Audit of Information Systems and Business Processes published in the Official Gazette of 31 January 202, regulates the procedures and principles regarding the auditing of the information systems and business processes of the institutions under the supervision and control of the Banking Regulation and Supervision Agency by independent audit firms authorised within the scope of this Regulation.

According to the Regulation on Bank Information Systems and Electronic Banking Services, customer data may not be transferred abroad without the explicit request of the customer. Owing to this regulation, the use of cloud computing services that have servers located abroad may be problematic in terms of banking services, as the use of cloud computing services with servers located abroad is regarded as data transfer abroad by Law No. 6698.

Pursuant to the Communiqué on Information Systems of Payment and Electronic Money Institutions and Data Sharing Services of Payment Service Providers in the Field of Payment Services (Communiqué) published in the Official Gazette of 1 December 2021; in the scope of the management of the outsourcing process for information systems, outsourcing service providers may provide outsourced services through the community cloud service model, in which hardware and software resources allocated only to payment service providers or other credit institutions or financial institutions whose activities related to information systems are regulated and supervised by a competent authority within the framework of the relevant legislation are physically shared but logically assigned a separate resource specific to each payment service provider.

Read this article on Lexology

The Communiqué stipulates that institutions may outsource services through the community cloud service model if such services are provided by external service providers deemed appropriate by the Central Bank of the Republic of Turkey (CBRT), and the CBRT is authorised to determine the appropriateness of external service providers that may offer external services through the community cloud service model.

Accordingly, the CBRT published the Guidelines on External Service Providers Offering Community Cloud Services (Guideline) in July 2022, which brings requirements on external service providers wishing to offer services through the community cloud service model.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Unlike common law jurisdictions that offer patent protection to software-implemented inventions and upon the fulfilment of certain criteria, even business methods, Turkey does not afford patent protection to software-implemented inventions and business methods. Copyright protection is the method that can be utilised for protecting the ownership of rights over software.

Original works that bear the characteristics and originality of the author are protected by copyright in Turkey, and these works are classified by Law No. 5846 of 5 December 1951 on Intellectual and Artistic Works as follows:

- science and literature;
- music;
- fine art; and
- cinema.

These categories are numerus clausus, and software is listed under the 'science and literature' category.

If a copyrighted work such as a piece of software is created, it is not compulsory to register it, and one owns the copyright and the protection at the time it is created or made public. Nevertheless, there is a non-compulsory registry system at the General Directorate of Copyright of the Ministry of Culture and Tourism that requires little proof. The general protection period is the lifetime of the author plus 70 years. There is no application similar to that of a patent application that is required of a copyright holder. Software and computer programs are classified under Class 9 of the Turkish Classification System published on the Turkish Patent and Trademark Authority's website; however, each piece of software may contain characteristics of more than one specific class and this should be taken into consideration.

While software generally falls under copyright protection, industrial property protection can also be provided under certain conditions. If a software that works or runs with a machine

or device, or is connected to a machine or device, the machine or system can be patented together with that device. Also, a computer program that performs a method that solves a technical problem can be protected by a patent. This protection is within the scope of Industrial Property Law No. 6769 and the Turkish Patent and Trademark Office is authorised to carry out the related transactions.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

In principle, pursuant to Industrial Property Law No. 6769, unless otherwise agreed upon due to special contracts made between the parties (employer and employee) or the nature of the work, the rights to designs made by employees shall belong to the employer according to employees' job descriptions and obligations arising from the labour contract or owing to the experiences and operations of the business organisation. For an invention to qualify as an 'employee service invention', it must be realised during the course of employment. The employee is obliged to report the invention to his or her employer in writing without delay. Additionally, free inventions that are the employee's inventions outside the scope of employee service inventions are also subject to reporting obligations for employees, who must make a declaration of the invention to their employer if the invention is made during their employment contract.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Certain restrictions and joint ownership provisions exist, both for copyright and patents. For copyright, joint ownership provisions and restrictions find form within the Law on Intellectual and Industrial Rights (Law No. 5846). For patents, Law No. 6769 provides that joint ownership is permissible and imposes restrictions upon the patent holders of intellectual property (IP) rights. Pursuant to Law No. 6769, if an invention is made by more than one person, each of the inventors may apply for a patent and these inventors shall be granted joint ownership.

If the design application or design belongs to more than one person, the partnership claim on the right shall be determined pursuant to the agreement concluded between the parties, and if there is no such agreement between the parties, it is determined in accordance with the provisions related to joint ownership in Turkish Civil Code No. 4721. For a patent licence to be granted to third parties in relation to the use of an invention, each of the right owners must grant permission unanimously. Even in the case of joint ownership, the rights of the owners may not be separated in relation to a patent application or patent assignment. Additionally, in the case of joint ownership, the right owners may assign a joint representative.

Finally, according to Law No. 5846, if a work is created by more than one author and if the work is of an inseparable nature, joint ownership shall be assumed and the provisions regarding ordinary partnerships stipulated under Turkish Obligations Law No. 6098 shall apply.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Trade secrets are protected under several Turkish regulations, including the Turkish Criminal Code. Duties of confidentiality are established for a variety of parties, including but not limited to, board members, shareholders, proxies, auditors, employees and contractors. Trade secrets, such as technical production secrets, production methods, and research and development plans, are also protected under Law No. 6769.

According to Turkish Commercial Law No. 6102, the protection of trade secrets is stipulated as unfair competition, and persons that act in violation of the confidentiality obligation regarding trade secrets and disclose trade secrets in bad faith; and employees, representatives and other contractors that deceive employers into providing trade secrets, shall be subject to an administrative sanction or imprisonment of up to two years. In addition, pursuant to this Law, employers may request pecuniary and non-pecuniary damages from persons that violate the confidentiality obligation and non-competition obligation, causing unfair competition.

As for the protections offered during litigation processes where court records become public knowledge, the Turkish Civil Procedure Code shall apply. Pursuant to Law No. 6100, parties that act in bad faith and unreasonably utilise litigation proceedings to have access to trade secrets shall be subject to part of a whole retainer fee in addition to a disciplinary fine.

Additionally, pursuant to the Amendment to the Banking Law published in the Official Gazette of 25 February 2020, save for the mandatory provisions of the relevant legislation, customer information has been specified as 'customer secret' and the criteria regarding processing and transfer of said information shall be realised in accordance with the Personal Data Protection Law (Law No. 6698). Customer secrets will not be shared with or transferred to third parties in Turkey and abroad, except for exceptional cases specified in the Banking Law. Even in cases where the client grants explicit consent regarding the processing of his or her personal data, said data may not be transferred or shared domestically or abroad without the explicit request or order of the client.

The Regulation on the Sharing of Confidential Information (the Regulation) has been published in the Official Gazette of 4 June 2021. Also referring to Law No. 6493, the Regulation is aimed at determining the scope, procedures and principles of the sharing and transfer of bank secrets and customer secrets. With the Regulation, it has become mandatory for banks to establish an information-sharing committee. The committee shall be responsible for coordinating the sharing of customer secrets and bank secrets.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

There are no specific regulations on IP protection regarding fintech innovations. Intellectual and industrial property rights are generally protected by Law No. 5846 on Intellectual and Artistic Work and Law No. 6769. If fintech products or services are subject to industrial property rights (namely, a trademark or patent), a patent or trademark is required to be registered before the Turkish Patent and Trademark Office. However, there is no registration requirement in terms of intellectual rights.

According to Law No. 5846, ownership of a fintech innovation will belong to its first creator and he or she will be deemed an author. If an employee creates an innovation during the employment contract, the author will be his or her employer. The duration of the IP right is the life of the author plus 70 years.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

According to Law No. 5846, authors whose IP rights have been violated may:

- file a civil lawsuit regarding the prohibition of the infringement;
- file a civil lawsuit regarding the prevention of infringement;
- request compensation; or
- file a criminal lawsuit.

According to Law No. 6769, persons whose rights are being violated may:

- file a civil lawsuit regarding probable infringement;
- file a civil lawsuit to cease infringement;
- file a civil lawsuit regarding the removal of infringement and request compensation; or
- request for necessary precautions to be taken.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

There are significant duties levied upon financial institutions regarding the duty of confidentiality within Turkish legislation, namely the Banking Law, the Turkish Commercial Code, the Turkish Criminal Code and the Personal Data Protection Law. This duty limits the sharing of data in a manner that would be considered as promoting competition. The Report

on Financial Technologies in Payment Services, which was published on 8 December 2021, emphasised the importance of making maximum use of the radical transformation in the financial sector in Turkey and revealed the necessity of interinstitutional cooperation in this field focused on the issues supporting the development of financial technologies, exclusionary actions of established enterprises, regulatory framework, market dynamics and market entry of large technology companies.

Also, pursuant to Communiqué No. 2022/2 on the Amendment of Communiqué No. 2010/4 (Communiqué No. 2010/4) on the Mergers and Acquisitions Subject to the Approval of the Competition Board (the Amendment Communiqué) published in the Official Gazette of 4 March 2022, the Turkish merger control thresholds have been raised and those exceeding certain thresholds will have to obtain permission from the Competition Board. However, the Competition Authority has clarified that it wishes to review the transactions of fintech and software companies as well as digital platforms regardless of whether they exceed the set thresholds or not.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

There exists a variety of tax incentives that are applicable to entities that are active in the technology industry, albeit these incentives are not exclusive to the fintech industry and under most circumstances, an entity's entitlement to these incentives requires that a sectoral analysis of the applicant be performed on a case-by-case review.

According to Law No. 4691 on Technology Development Zones, the fintech companies located in technoparks can benefit from numerous tax incentives, including exemption from corporate tax, income tax and value added tax. The exemption application for the research and development design and support personnel working in the Technology Development Zone was amended with the Amendment Law on Technology Development Zones, which was published in Official Gazette No. 31384 of 3 February 2021. In parallel with the practice implemented in research and development centres, the minimum living allowance is arranged in such a way that the remaining tax amount after deducting the tax corresponding to the minimum wage exemption is deducted from the tax accrued on the concise declaration to be submitted. Further, under the same law, a taxpayer whose primary place of business is located within a designated tech zone shall be excluded from the duty of paying corporate tax and income tax until 31 December 2028 with the Amendment Law.

According to Presidential Decree No. 2834, published in the Official Gazette of 8 August 2020, the rate of bank and insurance transactions tax (BITT) is applied as five per cent in foreign exchange sales to foreign resident organisations that perform at least one of the activities accepted as a financial institution activity in accordance with Banking Law No. 5411.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

A new digital service tax was introduced with the Law on the Digital Service Tax and Amendments on Certain Laws and Decree No. 375, published in the Official Gazette of 7 December 2019. Revenue gained from the activities that fall under the definition of digital services and intermediary services provided in the digital environment shall be subject to digital service tax. Taxpayers exceeding a revenue threshold of €750 million in global revenue and 20 million Turkish liras in local revenue will be subject to a digital service tax at a rate of 7.5 per cent.

Also, the transactions carried out by the fintech companies that fall within the scope of the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions are subject to BITT at a rate of 5 per cent in general (although some transactions are subject to 1 per cent or zero per cent BITT).

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

There is no specific immigration scheme for fintech businesses to recruit staff from abroad. However, in the Turkish legal framework, there are several laws and regulations for immigration schemes to recruit skilled staff from abroad.

The main regulations are:

- the Turkish Citizenship Law;
- the Law on Foreigners and International Protection;
- the International Labour Law;
- the Law on Work Permits for Foreigners; and
- the Law on Residence and Travel of Foreigners in Turkey.

Persons that provide significant investment and employment opportunities or are expected to provide significant improvements to the technology and sciences sector, can receive Turkish citizenship under the Turkish Citizenship Law.

As for work permits, industries that require specific expert employment or a qualified executive candidate be appointed to director positions, auditor positions that require the supervision of technical and administrative standards, or any other personnel that might be classified as key personnel will be eligible to receive a residency and work permit.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

A developing fintech industry exists in Turkey. Pursuant to the Turkey Fintech Guide 2023, published by the Presidency of the Republic of Turkey Finance Office, Turkey has received a start-up investment of US$1.6 billion in 2022, ranking 10th in Europe and third in the MENA, which was invested in 300 start-ups, out of which the fintech industry received the highest number of investments with 34 deals.

As a significant development, the Regulation Amending the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism (Decision No. 6702) was published, and the limit for certain institutions such as banks, institutions other than banks authorised to issue debit cards or credit cards, financing and factoring companies and financial leasing companies' obligation to check their customers' identities has been raised to 185,000 Turkish liras or more.

As per developments on asset management companies, the Communiqué on Portfolio Management Companies and Activities of Such Companies (III-55.1) issued by the Capital Markets Board has been amended as per the Communiqué (III-55.1.d) (Amending Communiqué), published in the Official Gazette of 18 February 2023. The Amending Communiqué introduced the concept of sub-portfolio management, which includes a contract to be signed between institutions or asset management companies authorised for portfolio management abroad for sub-portfolio management. Within the framework of this agreement, it refers to the activity of managing a certain portion or all of the portfolio of the portfolio manager by the sub-portfolio manager.

In terms of artificial intelligence (AI), the Regulation on the Structure and Activities of the Türkiye Health Data Research and Artificial Intelligence Applications Institution was published in the Official Gazette of 12 March 2022. With the Regulation, the establishment, structure, duties, authorities, working principles and procedures of the Türkiye Health Data Research and Artificial Intelligence Applications Institute have been regulated. This Regulation aims to increase the use of health data and AI in Turkey as well as conducting and supporting scientific and technological research in this context; and provide financial or scientific support to, coordinate and monitor research and development activities to be carried out on the use of AI and health data.

Another important development in Turkey's fintech ecosystem is regarding the insurtech field. The Regulation on the Provision of Remote Health Services (Regulation), which entered into force upon its publication in the Official Gazette of 10 February 2022, regulates the procedures and principles regarding the scope of remote health services, the authorisation of healthcare facilities that will provide remote health services, the development and registration of remote health information systems, and the inspection of healthcare facilities within this scope.

There were also developments in the cloud computing area. Pursuant to the Communiqué on Information Systems of Payment and Electronic Money Institutions and Data Sharing

Services of Payment Service Providers in the Field of Payment Services, the Central Bank of the Republic of Turkey published the Guidelines on External Service Providers Offering Community Cloud Services (Guideline) in July 2022, which brings requirements on external service providers wishing to offer services through the community cloud service model.

Last, The Banking Sector Good Practices Guide on the Protection of Personal Data was published by the Personal Data Protection Authority on 5 August 2022, specifically on the subject of open banking systems. The Guide contains general explanations regarding the procedures and principles that banks must comply with in the field of personal data protection and the obligations to be fulfilled.

Cigdem Ayozger Ongun cigdem@srp-legal.com
Deniz Erkan deniz.erkan@srp-legal.com

Sakayikli Sokak No: 10, Levent 34330, Istanbul 34330, Turkey
Tel: +90 212 401 44 01
www.srp-legal.com

Read more from this firm on Lexology

Read this article on Lexology

United Arab Emirates

Raza Rizvi and Muneer Khan
Simmons & Simmons

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 630
General innovation climate 630
Government and regulatory support 632

FINANCIAL REGULATION 633
Regulatory bodies 633
Regulated activities 633
Consumer lending 635
Secondary market loan trading 636
Collective investment schemes 636
Alternative investment funds 637
Peer-to-peer and marketplace lending 637
Crowdfunding 638
Invoice trading 638
Payment services 639
Open banking 640
Robo-advice 640
Insurance products 641
Credit references 641

CROSS-BORDER REGULATION 642
Passporting 642
Requirement for a local presence 642

SALES AND MARKETING 643
Restrictions 643

CRYPTOASSETS AND TOKENS 643
Distributed ledger technology 643
Cryptoassets 645
Token issuance 647

ARTIFICIAL INTELLIGENCE 649
Artificial intelligence 649

CHANGE OF CONTROL 650
Notification and consent 650

Read this article on Lexology

FINANCIAL CRIME 650
Anti-bribery and anti-money laundering procedures 650
Guidance 651

DATA PROTECTION AND CYBERSECURITY 652
Data protection 652
Cybersecurity 654

OUTSOURCING AND CLOUD COMPUTING 655
Outsourcing 655
Cloud computing 655

INTELLECTUAL PROPERTY RIGHTS 656
IP protection for software 656
IP developed by employees and contractors 656
Joint ownership 657
Trade secrets 657
Branding 658
Remedies for infringement of IP 658

COMPETITION 659
Sector-specific issues 659

TAX 659
Incentives 659
Increased tax burden 659

IMMIGRATION 659
Sector-specific schemes 659

UPDATE AND TRENDS 660
Current developments 660

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

There is a progressive and ambitious vision around fintech innovation in the UAE, with some fintech subsectors generating more notable and scaled innovation than others. Government and public-sector entities and regulators play a key role in the innovation strategies across most industry verticals and this is also the case for fintech. From a financial services regulatory perspective, the UAE comprises three separate and independent jurisdictions:

- the Dubai International Financial Centre (DIFC);
- the Abu Dhabi Global Market (ADGM); and
- the remainder of the UAE (often referred to as 'onshore' or 'onshore UAE').

Federal-level financial services regulators have jurisdiction over onshore UAE; however, the DIFC and the ADGM each have their own regulatory bodies, and all the various regulators

across all three jurisdictions have identified fintech innovation (albeit with some different flavours) as a key priority.

In the DIFC, the DIFC FinTech Hive runs a now well-established accelerator programme that has focussed on fintech, insurtech, regtech and Islamic fintech start-ups. In tandem, the DIFC's financial services regulator, the Dubai Financial Services Authority (DFSA) launched its Innovation Testing Licence (ITL), a regulatory sandbox in 2017. These initiatives are in line with the goals of the Dubai Plan 2021 strategy to develop Dubai's economy. The DFSA has also signed a number of bilateral fintech agreements with other regulators globally, such as with the Monetary Authority of Singapore in August 2018 and Japan's Financial Services Agency in September 2018, to cooperate in the development of fintech and to foster innovation in their respective jurisdictions. Other similar agreements that the DFSA has entered into include with the Australian Securities and Investment Commission, the Hong Kong Monetary Authority, the Hong Kong Securities and Futures Commission, the Hong Kong Insurance Authority and the Securities Commission Malaysia.

In 2023, the DIFC introduced the DIFC Launchpad as the world's first venture studio platform exclusively focused on promoting the growth of innovative start-ups and scale-ups in the region. To accompany this initiative, the DIFC introduced the Venture Studio Regulations as the first global legal framework for the venture-building model.

Similarly, the ADGM's financial services regulator, the Financial Services Regulatory Authority (FSRA) launched its regulatory sandbox, the Regulatory Laboratory (RegLab) following the implementation of its fintech legislative framework. The ADGM has also partnered with the Association of Southeast Asian Nations Financial Innovation Network, which launched a digital marketplace – the Application Programming Interface Exchange (APIX) – for South-East Asia to support financial inclusion, to test the cross-border connectivity between the ADGM Digital Sandbox and APIX.

Both the DFSA and the FSRA are members of the Global Financial Innovation Network (GFIN), to, among other objectives, assist with cross-border testing of fintech solutions.

Beyond the DIFC and ADGM financial free zones, there are a number of other initiatives to foster innovation in the UAE that cross over into the UAE fintech sector. Additionally, the Smart Dubai initiative is the Emirate of Dubai government office charged with facilitating Dubai's citywide smart transformation, to empower, deliver and promote an efficient, seamless, safe and impactful city experience for residents and visitors. Among its key initiatives are the development of Dubai's first Artificial Intelligence Smart lab and the Dubai Blockchain Strategy, which is a collaboration between the Smart Dubai Office and the Dubai Future Foundation to continually explore and evaluate the latest technology innovations. The UAE created the first Minister of Artificial Intelligence with a mandate that will cross over into fintech innovation.

In May 2021, another key freezone, the Dubai Multi Commodities Centre (DMCC) launched the DMCC Crypto Centre to provide an ecosystem for businesses operating in the cryptographic and blockchain sectors. The DMCC inked a memorandum of understanding with the UAE Securities and Commodities Authority (SCA) to provide a regulatory framework for crypto-related businesses. Following on from this, it should be noted that 2022 was a hugely

Read this article on Lexology

significant year for the UAE's crypto ambitions with the introduction of the Virtual Assets Regulatory Authority as the world's first independent regulator for virtual assets.

In February 2023, the UAE Central Bank issued a press release announcing the launch of the Financial Infrastructure Transformation (FIT) Programme to promote the digital transformation across the financial services sector in the region. The FIT Programme is set to be integrated by 2026 and is divided into nine key pillars, one being central bank digital currency (CBDC). This initiative is part of the first stage of the implementation of the programme, which aims to develop a number of digital payment infrastructures and services such as the issuance of CBDCs for cross-border and domestic uses. According to the press release, by doing this the UAE Central Bank aims to improve the inefficiencies of domestic payments.

This and other notable initiatives around crypto, digital assets and other payments innovation geared towards supporting the UAE's Web 3.0 ambitions reinforce the widely held view that in this region, the UAE is breaking new ground in fintech innovation.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

The UAE's financial services free zones (namely, the ADGM and the DIFC) each have their own regulators that have launched initiatives to enable fintech businesses to participate and test their solutions in environments with lighter-touch regulation.

In the ADGM, the FSRA has created a RegLab. Participants in the RegLab are not subjected to the full suite of authorisation regulations and rules from the outset; rather, a customised set of rules will be applied, which will depend on the business model, the technology deployed and the risk profile of the fintech participant.

Under the RegLab framework, fintech participants are given two years to develop, test and launch their products and services in a controlled environment, after which fintech participants with viable business models will be transferred to the full authorisation and supervisory regime (provided they meet the authorisation criteria). Firms that are not ready after the two-year period will exit the RegLab framework.

In the DIFC, the DFSA has created the ITL, which fintech companies can apply for to test an innovative product or service for six to 12 months. In exceptional cases, the DFSA will consider extending that period. If an ITL licensee has met the outcomes detailed in its regulatory test plan, and it can meet the full DFSA authorisation requirements, it will migrate to full authorisation. If it does not, the company will have to cease carrying on activities in the DIFC that need regulation. The DIFC also launched a fintech fund of US$100 million fund with a stated objective to help promising start-ups raise growth capital, while also supporting their outreach and connections within the wider financial services industry.

To further the ambition of innovation of Dubai and the UAE in the financial world, the DFSA and the FSRA are committed to cross-border testing under the direction of the GFIN. The purpose of such a pilot scheme is to assist in providing efficient ways for fintech firms to engage with regulators across multiple jurisdictions.

Read this article on Lexology

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

For banking and lending-related activities in onshore UAE, the financial services regulator is the UAE Central Bank, while for securities and capital markets-related matters, the UAE Securities and Commodities Authority (SCA) is the relevant regulator. Following the merger between the UAE Central Bank and the UAE Insurance Authority under Decretal Federal Law No. 25 of 2020, the UAE Central Bank is now also the Onshore UAE insurance sector regulator.

In February 2022, Law No. 4/2022 Regulating Virtual Assets in the Emirate of Dubai (the Dubai Virtual Assets Law), creating the Virtual Assets Regulatory Authority (VARA), was passed. VARA regulates businesses relating to virtual assets, including cryptoassets and non-fungible tokens (NFTs) in the Emirate of Dubai including all special development zones and free zones in Dubai, other than the Dubai International Financial Centre (DIFC). Since VARA's introduction, it has enacted the Virtual Assets and Related Activities Regulations 2023 (the Virtual Assets Regulations), establishing a central legal framework for virtual asset service providers (VASPs) to advance VARA's regulatory objectives in Dubai's virtual assets space.

For all regulated financial activities in the DIFC, the regulator is the Dubai Financial Services Authority (DFSA). For all regulated financial activities in the Abu Dhabi Global Market (ADGM), the regulator is the Financial Services Regulatory Authority (FSRA).

It should also be noted that the UAE Central Bank established the FinTech Office, following its announcement at the FinTech Abu Dhabi 2020, to foster the development of the fintech sector, placing the country at the forefront of the market. However, it is important to highlight that the FinTech Office's aim is to embrace innovation and digital transformation but does not have its own regulatory mandate and has no regulatory purposes.

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

The onshore UAE regulatory regime is separate and different from the regulatory regime found in the DIFC and the ADGM. So, when considering the UAE, it is important to first ask which specific jurisdiction and financial regulatory regime is applicable.

As financial free zones, both the DIFC and the ADGM have their own common law-based commercial and civil legal and financial services regulatory frameworks, as well as their own dedicated courts. The DFSA is the financial services regulator for activities conducted in or from the DIFC and the FSRA regulates financial services activities in or from the ADGM. The relevant federal onshore UAE (namely, in the UAE but outside the DIFC and ADGM) financial regulators are the SCA and the UAE Central Bank. The UAE Central Bank is the prudential regulator for onshore UAE and mainly regulates activities relating to banking and lending activities such as:

Read this article on Lexology

- deposit-taking (including sweep deposit accounts);
- foreign exchange trading;
- guarantees and commitments;
- payment services (including the issuance of payment instruments and other means of payments);
- primary lending;
- factoring;
- invoice discounting;
- arranging primary loans;
- secondary market loan trading; and
- secondary market loan intermediation.

Outside the banking and lending context, the UAE Central Bank was historically the sole financial services regulator for onshore UAE prior to the establishment of the SCA (in 2001) and the UAE Insurance Authority (IA) (in 2007). However, the IA has now been absorbed by the UAE Central Bank. There are therefore some other areas of financial activity that the UAE Central Bank continues to regulate – such as, among other things, currency brokerage, money exchange and some activities that would be typically associated with investment banking.

Generally, the types of regulated activities in onshore UAE, the DIFC and the ADGM include, among other things:

- the marketing and sale of securities;
- providing investment advice;
- dealing in products and investments (either as principal or agent);
- underwriting and placing financial products;
- offering and providing discretionary investment management services;
- marketing or selling funds (including the provision of investment advice);
- accepting deposits;
- providing credit;
- providing money services;
- arranging deals in investments;
- managing assets;
- managing a collective investment fund;
- advising on financial products; and
- insurance intermediation.

Securities and financial products that are regulated by the respective financial services regulators across onshore UAE, the DIFC and the ADGM include, but are not limited to, equity securities, debt securities, linked products, derivatives, structured products, deposits, notes and warrants.

The Securities and Commodities Authority Decision No. 23/RM/2020 Concerning Crypto Assets Activities Regulation (the Crypto Assets Regulation) establishes a regime for crypto trading within the UAE. The Crypto Assets Regulation is applicable to exchanges, crowdfunding platforms and other related financial services based on leveraging cryptoassets. The following are considered to fall under the ambit of the Crypto Assets Regulation:

Read this article on Lexology

- promoting, offering or issuing cryptoassets in the UAE;
- providing cryptoasset custody services, operating an exchange for cryptoassets or operating a crypto fundraising platform in the UAE; and
- carrying on any other financial activities relating to cryptoassets such as promotion and marketing, issuance and distribution, advice, brokerage, custody and safekeeping, fundraising and operating an exchange.

More recently, VARA imposes the obligation to obtain an express authorisation from VARA when carrying out seven virtual asset activities, including:

- advisory services;
- broker-dealer services;
- custody services;
- exchange services;
- payments and remittances services;
- management and investment services; and
- transfer and settlement services.

VASPs that fulfil VARA's licensing requirements are also required to comply with activity-specific rulebooks (in addition to the five VARA compulsory rulebooks) relating to their provision of the relevant virtual asset activities.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Yes. Article 65 of UAE Decretal Federal Law No. 14 of 2018 Regarding the Central Bank and Organisation of Financial Institutions and Activities provides that the UAE Central Bank will regulate, among other things, the activities of 'providing credit facilities of all types', 'providing stored values services, electronic retail payments and digital money services' and 'providing virtual banking services'.

With regard to the provision and booking of these services 'in or from' either the DIFC or the ADGM, these activities are likely to be considered as 'providing credit', which will require a licence from either the DFSA or FSRA respectively. To the extent that these services are only 'advised' on or 'arranged' from the same jurisdictions, an appropriate licence would also be required from either the DFSA or FSRA. If these services are merely promoted (with no 'advising' or 'arranging') 'in or from' either financial free zone, unless an exemption applies, a Representative Office licence would be required from either the DFSA or the FSRA respectively.

In November 2020, the UAE Central Bank issued the Consumer Protection Regulations 2020 to ensure the protection of consumers' interests in their use of any financial product, service or relationship with licensed financial institutions. This ensures that the licensed financial institutions' approach to consumer protection is in line with international standards. Along with the objective of promoting a culture within licensed financial institutions of respecting and acting in the best interest of consumers, it specifically aims to protect consumers by defining the institutional obligations for the protection of consumers.

Read this article on Lexology

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

Secondary market loan trading is an activity regulated by the UAE Central Bank. It constitutes primary lending and is regulated whether or not the loan has been fully drawn. The trading of loans would also constitute a regulated financial services activity in the DIFC and the ADGM.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

In onshore UAE, there is a general prohibition on marketing unregistered collective investment schemes (ie, funds) unless they have been registered with the SCA accordingly (either for private or public promotion). However, the onshore UAE marketing prohibition does not apply to the promotion of foreign funds to a non-natural 'qualified investor'. A non-natural qualified investor is defined in the SCA rules and includes the federal government, among others.

There is a private placement regime under the SCA rules, where if the potential investor is a natural person, foreign funds can be registered for private placement by an SCA-licensed promoter subject to several conditions.

With regard to the DIFC, there is a prohibition on marketing unregistered funds in the DIFC except through a DFSA-licensed intermediary with the appropriate type of licence, unless an exemption applies. The prohibition on the offer or sale of a fund only applies where this activity is carried out 'in or from' the DIFC. It is not possible to register a foreign fund for distribution in the DIFC. Funds need only be registered with the DFSA if they are domiciled in the DIFC. There are currently relatively few funds domiciled in the DIFC and so most funds marketed in the DIFC are foreign (ie, non-DIFC-domiciled) and, therefore, unregistered. However, all funds and collective investment schemes promoted 'in or from' the DIFC need to meet a fund eligibility criteria.

Once a marketing entity holds the appropriate licence it may market foreign-domiciled funds or DIFC-domiciled funds, provided it markets only to investors within the scope of its licence, and in the case of any foreign fund:

- the fund qualifies as a 'designated' or 'non-designated fund';
- the marketing entity has a reasonable basis for recommending a fund as suitable to a particular client; or
- the fund offered discreetly to persons who are professional clients and the minimum subscription per investor is US$50,000.

Similar provisions exist with regard to the ADGM.

Read this article on Lexology

Following a public consultation, the DFSA updated its rules to include 'operating a crowdfunding platform' as a regulated activity.

With regard to onshore UAE, Circular No. 7/2020, the Loan-Based Crowdfunding Activities Regulation, was published in October 2020 by the UAE Central Bank. This regulates the operation of crowdfunding companies, platforms, borrowers, lending and controls over client money. The regulation sets out rules on the requirements for entities that can be involved in such regulated activities and the segregation of crowdfunding money to be held within UAE banks with such accounts being required to be audited regularly.

However, depending on the specific activities undertaken (ie, where the platform merely introduces two independent contracting parties or if the platform is actively establishing a fund or offering securities), the activity may potentially fall under existing UAE Central Bank or SCA regulation.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Yes, managers of alternative investment funds are regulated in onshore UAE, the DIFC and the ADGM.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Lending is a regulated activity whereby intermediary platforms are required to obtain approvals to operate from the UAE Central Bank, which would trigger compliance requirements on the platform including the proper vetting of borrowers and anti-money laundering checks.

While interest is prohibited under articles 458 to 459 of Federal Decree-Law No. 31/2021 On the Issuance of the Crimes and Penalties Law and is void under articles 204 and 714 of the Civil Code, interest is permitted under articles 72 of the Commercial Code, provided it does not exceed 9 per cent. In any case, UAE Federal Supreme Court Decision No. 14/9 of 28 June 1981 permits the charging of simple interest (presumably as opposed to compound interest) in connection with banking operations.

On 1 August 2017, changes to the DFSA rules came into force that introduced rules relevant to crowdfunding. Additional rules, which included investment limits and property valuation requirements in the context of property crowdfunding, came into force on 1 July 2019.

In September 2018, the ADGM launched the Guidance on the Regulatory Framework for Private Financing Platforms after holding a consultation on the matter. This framework intends to regulate operators of private financing platforms serving equity investment, debt financing and trade receivables funding needs of start-ups, private enterprises and small and medium-sized enterprises (SMEs). It contains rules on loan-based or investment-based

crowdfunding, which affects private financing platform operators that seek to connect clients or investors to their stakeholders

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

Financial services in the UAE are regulated either by the UAE Central Bank or the SCA depending on the nature of the activity. In respect of financial free zones in the UAE, such activities are regulated by the DFSA in the DIFC, and the FSRA in the ADGM. In particular, issues of securities by UAE companies are regulated under the UAE Companies Law (Federal Law No. 2 of 2015) (as amended by Federal Decree-Law No. 26/2020 on the amendment of certain provisions of Federal Law No. 2/2015 on Commercial Companies) and regulations issued by the SCA. As such, under the UAE Companies Law, only public joint-stock companies may offer securities by way of a public subscription through a prospectus. Other companies, whether incorporated in the UAE (onshore or in a free zone) or in a foreign jurisdiction, are prohibited from advertising including the invitation to a public subscription without the approval of the SCA. In practice, private joint-stock companies are entitled to issue securities to sophisticated investors by way of a private placement. Accordingly, this regulatory limitation restricts the ability of limited liability companies, the legal form adopted by most SMEs in the UAE, from raising funds through equity-based crowdfunding.

In recent times, changes to the DFSA rules came into force that introduced rules relevant to crowdfunding. Additional rules, which included investment limits and property valuation requirements in the context of property crowdfunding, came into force on 1 July 2019.

The FSRA previously issued the Guidance on Regulatory Framework for Private Financing Platforms, which seeks to regulate crowdfunding activities aimed at private companies (start-ups to SMEs) to source alternative financing from private and institutional investors. Regulatory requirements include capital requirements, risk analysis, due diligence, marketing restrictions and limits on exit options.

The UAE Central Bank has published Circular No. 7 of 2020 Loan-Based Crowd Funding Activities Regulations containing a framework for licensing, regulating and monitoring load-based crowdfunding platforms (CFPs), safeguarding the financial system from the risks posed by such platforms, assisting in administering the loans resulting from CFP operations as well as to safeguard the interests of the consumers in the UAE.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

Invoice trading currently falls within the activity of 'arranging credit' within the DIFC and is regulated as such by the DFSA. Similar provisions exist in the ADGM. With regard to onshore UAE, invoice trading will require a form of regulatory licence either from the UAE Central Bank (if its activities fall under Federal Decree-Law No. 16/2021 on Factoring and Transfer of Civil Accounts Receivable) or the SCA (if invoices were to be considered as a financial product falling within the SCA's Promoting and Introducing Regulations – Regulation 3/RM

of 2017). To the extent that services are merely promoted within onshore UAE, the DIFC or the ADGM, a Representative Office licence in the respective jurisdiction would be required.

Payment services

12 | Are payment services regulated in your jurisdiction?

Yes. In 2017, the UAE Central Bank published its Regulatory Framework for Stored Values and Electronic Payment Systems, which singularly covered digital payment services.

This has since been replaced by the UAE Central Bank's Stored Value Facilities Regulation (the SVF Regulation), issued in September 2020. In addition, the UAE Central Bank issued the Retail Payment Systems Regulation (the RPS Regulation) and the Large Value Payment Systems Regulations (the LVPS Regulation) in January 2021. Further, the Retail Payment Services and Card Schemes Regulation (the RPSCS Regulation) was issued in July 2021. Together, the four regulations now cover the regulatory framework for payment system providers in the UAE (the Payment Services Regulations).

The SVF Regulation covers the licensing, enforcement and supervision of SVF in the UAE as well as non-UAE entities that promote SVF on a cross-border basis.

The RPS Regulation sets out the licensing, designation and oversight framework that the Central Bank intends to follow with respect to the licensing and designation of RPS. It aims to ensure the safety and efficiency and smooth and efficient operation of the financial infrastructure system.

The LVPS Regulation applies to LVPS operating in the UAE or those that accept clearing or settlement of transfer orders denominated in the UAE dirham both within the UAE and outside. The LVPS Regulation requires compliance with the provisions of the Principle of Financial Market Infrastructures. It also covers the licensing obligations and requirements in relation to LVPS as well as the ongoing requirements for designated LVPS.

The RPSCS Regulation sets out the rules and conditions for acquiring and maintaining a licence for the provision of retail payment services and operating a card scheme. The term 'retail payment services' comprises nine defined categories of retail payments services: payment account issuance services, payment instrument issuance services, merchant acquiring services, payment aggregation services, domestic and cross-border fund transfer services, payment token services, payment initiation services and payment account information services.

The Payment Services Regulations each point to various other UAE Central Bank instruments and should therefore be considered in a wider context.

In the DIFC, following the publication of the DFSA's Consultation Paper No. 125 on Proposals for Money Services in 2019, the DFSA Rulebook Conduct of Business Module (COB Module) was amended to introduce requirements for the provision of money services in relation to electronic money in the DIFC.

Read this article on Lexology

The FSRA issued enhancements to its Regulations and Rules concerning providing money services (PMS) in November 2020. The improvements include amendments to the scope of PMS as well as the introduction of a new set of rules in the FSRA's COB Rulebook for payment accounts and stored value services as well as more risk-sensitive capital requirements for such services.

The recent Virtual Assets Regulations also provide 'payment and remittances services' as one of the seven virtual assets activities covered by the new regulations. All VASPs operating in Dubai must now be licensed by VARA and must also comply with the compulsory and activity-specific rulebooks. The payments-related rulebook was published in June 2023.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

Other than in the context of a regulatory or official investigation, there is no specific obligation in UAE legislation requiring the disclosure of data to third parties.

The general position is that financial institutions that are in a position to collect and store data from the public are bound by a duty of confidentiality. A breach of this duty of confidentiality could attract criminal liability under article 432 of the UAE Penal Code. Further, article 106 of the Banking Law requires the UAE Central Bank to keep confidential all banking data that it receives.

In February 2023, the Central Bank of the UAE issued a press release announcing the launch of the Financial Infrastructure Transformation (FIT) Programme to promote the digital transformation across the financial services sector in the region. The FIT Programme is set to be integrated by 2026 and is divided into nine key pillars, one being open finance. This initiative is part of the second stage of the implementation of the programme, which aims to develop a number of digital infrastructures, including the establishment of open finance platforms to foster cost-efficiency, innovation, customer experience and improve regulatory compliance security and operational resilience. In particular, by developing open finance infrastructures, the UAE Central Bank wishes to strengthen collaboration in the financial services sectors through interconnectivity and interoperability among all players and institutions.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

The FSRA has issued a regulatory framework for digital investment managers (robo-advisers) operating in the ADGM. To supplement this, the FSRA has also released guidance to illustrate how its regulatory framework applies to robo-advisers in the ADGM. In particular, the guidance outlines:

- the regulatory permission that may be required to provide digital investments services in or from the ADGM; and
- how the FSRA will apply its authorisation criteria in key existing areas of technology governance, suitability and disclosure, and newer areas such as algorithm governance.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Nothing in current DIFC or ADGM legislation specifically regulates fintech companies that wish to sell or market insurance products, and, therefore, the general regulation around the sale and marketing of insurance products in the relevant jurisdictions applies.

Insurance operations in onshore UAE are now regulated by the UAE Central Bank following the merger between the Insurance Authority and the UAE Central Bank under Federal Decree-Law No. 25 of 2020. The UAE Central Bank has assumed regulatory, supervisory, licensing and enforcement functions for the insurance sector.

The Electronic Insurance Regulations 2020 (Insurance Authority Board of Directors' Resolution No. 18 of 2020) was introduced to regulate insurance agents, actuaries, brokers, surveyors and insurance consultants carrying out insurance activities via electronic operations. Prior approval must be obtained to conduct insurance activity electronically and requires a raft of safeguards relating to electronic transactions including risk analysis and contingency plans for system disruptions.

The UAE Central Bank is committed to facilitating the advancements of new technologies across the financial sector as part of its fintech strategy. This includes adopting insurtech for insurance services.

Although the Insurance Authority and the UAE Central Bank have merged, the rules and regulations issued by the Insurance Authority under Federal Law No. 6 of 2007 will continue to apply to all licensed organisations until their replacement by the UAE Central Bank.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Yes. Pursuant to the SCA Board of Directors' Decision No. 18/RM of 2018 Concerning the Regulations as to Licensing Credit Rating Agencies, a credit rating is 'a periodic measure to determine and assess the ability of the rated entity to meet its financial liabilities, and potential risks that may affect it, and to evaluate the financial products and potential risks of acquiring them by the investor' and credit rating activities are regulated. To be eligible for a licence to carry on credit rating activities, an entity must have, among other things, a minimum of 2 million UAE dirhams in capital and consent from the UAE Central Bank (should the licence application be subject to their mandate).

In the DIFC, 'operating a credit rating agency' is a regulated activity that would require a DFSA licence. Similar provisions exist in the ADGM.

However, individual credit reference and information services are possible in the UAE through the Al Etihad Credit Bureau (AECB), which is a public joint stock company wholly owned by the UAE federal government. According to UAE Federal Law No. 6 of 2010 concerning Credit Information, the AECB is mandated to regularly collect credit information from financial and non-financial institutions in the UAE. The AECB aggregates and analyses this data to calculate credit scores and produce credit reports that are made available to individuals and companies in the UAE. The AECB collects information on individuals and companies from banks, finance companies and telecoms companies. Additional information from other sources such as utilities, real estate, government and other entities are planned to be added in the future. Financial institutions in the UAE are mandated by law to supply the AECB with all credit information on a monthly basis.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

In March 2019, the Emirates Securities and Commodities Authority, Financial Services Regulatory Authority (FSRA) and the Dubai Financial Services Authority (DFSA) announced that a new fund passporting regime would be available to facilitate the promotion of funds licensed by each authority across the UAE. The passporting of a UAE fund will allow the licensed firm to promote units to 'qualified investors' domiciled in the other relevant jurisdiction. A notification specifying to which other jurisdictions the fund is to be promoted needs to be given to the relevant regulator and the details of the passported UAE fund should be listed in the relevant regulators' Register of Passported Funds. This regime removes the need for multiple regulatory licences and reduces the costs for the promotion of funds across the UAE. The funds will still have to comply with the relevant requirements and the regulators have the power to take a fund off the Register of Passported Funds if they are non-compliant, wound up, or if one of the other regulators of fund managers requests that the fund be removed.

Other than in respect of funds, there is no passporting arrangement applicable to regulated activities although there is an industry desire to push for this and enable businesses to have wider reach.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

It is possible for fintech companies to market on a cross-border basis into onshore UAE without having to obtain a licence. If marketing activities are undertaken on a genuinely cross-border basis (namely, by telephone, website or email from outside the UAE) they should not be subject to UAE regulation. To ensure that marketing activities are conducted

on a true cross-border basis and not deemed to be conducting business in the UAE, several guidelines should be followed, which include not having a physical or legal presence in the UAE, marketing only towards non-natural qualified investors and making any subscription payments made outside the UAE.

In relation to cross-border marketing into the Dubai International Financial Centre (DIFC), there are several guidelines that should be followed to reduce the risk of marketing activities being treated as having taken place 'in' the DIFC, such as not having a physical or legal presence in the DIFC, keeping marketing materials generic and only made to certain types of pre-identified 'professional clients' (as defined under the DFSA's Conduct of Business Rules) and performing all generic marketing from outside the DIFC.

With regard to regulated activities where a licence is required from a UAE financial services regulator (including the UAE Central Bank, the Securities and Commodities Authority, the DFSA or the FSRA), a fintech company would need to be locally established in the relevant jurisdiction to obtain a licence. Note, however, that the initiatives launched by the Abu Dhabi Global Market and the DIFC require lighter regulatory oversight for qualified participants.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

There are a number of restrictions on the offering or promotion of financial services in onshore UAE, the DIFC and the Abu Dhabi Global Market, and in many cases corresponding exemptions relating to these promotions, all of which differ according to the type of product or service offered.

In February 2023, the new Virtual Assets and Related Activities Regulations 2023 issued by the Virtual Assets Regulatory Authority came into force, which imposes a number of restrictions on the sales and marketing of cryptoassets. This is mentioned in more detail in the Cryptoassets question of this chapter.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

The UAE federal government and certain emirate-level governments have publicly committed to the creation of problem statements and use cases to enable government services to benefit from distributed ledger technology (DLT) and, in particular, blockchain. Examples of this include the government of Dubai's public commitment to have all government services and transactions on the blockchain by 2020.

Read this article on Lexology

In some areas, UAE law is permissive as regards the use of DLT and distributed digital ledgers or databases in scenarios where parties intend to create legal relations; for example, article 12 of Federal Law No. 1 of 2006 on Electronic Commerce and Transactions, which seems to have foreseen 'smart contracts' by confirming the validity and enforceability of contracts formed through computer programs that include two or more electronic information systems present and pre-programmed to carry out the transaction, even if no individual is directly involved. The UAE government launched the Emirates Blockchain Strategy 2021, with the aim of transforming government transactions into the blockchain platform.

The Dubai Virtual Assets Law is designed to help regulate the operation of virtual asset platforms that utilise DLT. The Dubai Virtual Assets Law is applicable to the Emirate of Dubai including all special development zones and free zones in Dubai, other than the Dubai International Financial Centre (DIFC). The Virtual Assets Regulatory Authority (VARA) will be responsible for issuing licences for the provision of any virtual asset platform operation and management services. To date, only a handful of virtual asset service providers (VASPs) have demonstrated compliance with the VARA requirements and been granted licences in this regard – although it has been reported that hundreds of institutions are currently working to obtain licensing status.

The current VARA licence types that VASPs can seek to obtain are as follows:

- Preparatory Minimum Viable Product (MVP) Licence: VASPs must satisfy all of the licensing requirements under the VARA MVP Licence Conditions Document. The VASP must obtain an Operational MVP License before it can begin offering virtual asset services;
- Operational MVP Licence: VASPs that satisfy all of the operational requirements under the VARA MVP Licence Conditions Document. It allows VASPs to offer approved virtual asset services to institutional clients and qualified investors; and
- Full Market Product (FMP) Licence: VASPs must satisfy all of the requirements as specified under the Virtual Assets Regulations. It allows a VASP to offer approved virtual asset services to retail customers as well as institutional customers and qualified investors.

Only two VASPs to date have been granted Operational MVP licences. The remaining VARA licence recipients are currently at the MVP Provisional or MVP Preparatory stage. However, following the recent bankruptcies of renowned crypto institutions like FTX, those in the space have reported that VARA has tightened its licensing requirements and will likely be requesting additional information from applicants, thus presenting additional regulatory obstacles for prospective VASPs seeking licences in the near future.

In March 2021, the Dubai Financial Services Authority (DFSA) issued Consultation Paper No. 138 on the Regulation of Security Tokens (CP138). Although this proposal went through the consultation stages, it appears that no formal Feedback Statement was publicly released in this regard. As such, the DFSA launched a regulatory framework for investment tokens on the back of CP138 and updated its rulebook to reflect the same. Investment tokens are broadly defined as:

- a security or derivative in the form of a cryptographically secured digital representation of rights and obligations that is issued, transferred and stored using DLT or other similar technology; or

Read this article on Lexology

- a cryptographically secured digital representation of rights and obligations that is issued, transferred and stored using DLT or other similar technology and:

    - confers rights and obligations that are substantially similar in nature to those conferred by a security or derivative; or
    - has a substantially similar purpose or effect to a security or derivative.

In this regard, the marketing, issuing, trading or holding of investment tokens in or from the DIFC will be regulated.

Further, in April 2023, the Registration Authority (RA) of Abu Dhabi Global Market (ADGM), issued Consultation Paper No. 3 of 2023 to seek feedback on its proposal for a new legal framework for foundations that facilitate DLT and token issuance (the Distributed Ledger Technology Foundations Regulations 2023). The RA's key proposals include the structure of the DLT foundations, governance and control, tokens, reporting obligations, disclosures and publication, beneficial ownership, supervision, insolvency, liquidation or voluntary strike-off. The Distributed Ledger Technology Foundations Regulations 2023 are expected to be implemented shortly.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

The Stored Value Facilities Regulation allows the use of crypto or virtual assets as a stored value when purchasing goods and services. However, it was later clarified that such assets are not recognised legal tenders in the UAE, with the official legal tender being the UAE dirham. These assets may also be used as a form of investment and as such be subject to the UAE Securities and Commodities Authority (SCA) Regulations.

The SCA issued Board of Directors Decision No. 23/RM of 2020 Concerning the Regulation of Cryptoassets and Administrative Decision No. 11 of 2021 Concerning Guidance for Cryptoasset Regulations. The regulatory scheme aims to provide a licensing regime for the offering of cryptoassets in the UAE. The Decision defines cryptoassets as:

A record within an electronic network or distribution database functioning as a medium for exchange, storage of value, unit of account, representation of ownership, economic rights, or right of access or utility of any kind, when capable of being transferred electronically from one holder to another through the operation of computer software or an algorithm governing its use.

The regime also applies to security tokens and commodity tokens.

The Dubai Virtual Assets Law is also relevant to the regulation of virtual assets, which are broadly defined as 'a digital representation of the value that can be digitally traded or transferred or used as an instrument for exchange, payment or investment purposes'. This definition would therefore include cryptoassets such as security tokens, cryptocurrencies and NFTs. There is a general prohibition under the Dubai Virtual Assets Law preventing

entities from carrying out any virtual asset services to consumers unless they have received a licence from VARA, operate in Dubai and have a trade licence from the relevant commercial authority in Dubai. Applicants are currently granted an initial MVP licence by VARA, which allows them to provide products and services to select groups of investors, before they are fully authorised. Further details of the VARA licensing requirements are set out above. In August 2022, VARA enforced Administrative Order No. 1/2022 Relating to Regulation of Marketing, Advertising and Promoting Related to Virtual Assets (Marketing Regulations) to govern the promotion of virtual asset-related activities in Dubai (excluding the DIFC). To accompany this, VARA issued Administrative Order No. 2/2022, which lists certain fines and penalties for breaches of the Marketing Regulations. Relevant businesses will be liable to pay penalties ranging between 50,000 UAE dirhams to 200,000 UAE dirhams for independent offences, with fines being doubled (up to a maximum of 500,000 UAE dirhams) for repeat violations within the following year.

The ADGM regulatory framework for virtual assets (first introduced on 25 June 2018 and amended in February 2020) features a number of guidance points related to virtual assets and digital wallets.

In November 2019, the DFSA published Consultation Paper No. 125 on Proposals for Money Services. In the paper, the DFSA set out its proposal to allow certain activities relating to money services that have emerged owing to rapid advancements in technology, with the DFSA recognising that these activities could promote the growth of regulated financial services activities in DIFC and provide greater protection and choices to users of money services. One of the activities it proposed to allow was the provision of money services (as defined in the DFSA Rulebook Conduct of Business Module (COB Module)) in respect of electronic currency. Amendments to the DFSA Rulebook COB Module came into force on 1 April 2020, introducing requirements for the provision of money services in relation to electronic money in the DIFC.

More recently, in April 2023, the DFSA announced (through Consultation Paper No. 150) its plans to make several changes to the DFSA Rulebooks particularly to clarify elements of the money services, crypto tokens and crowdfunding regimes in the DIFC. It is also reported that the DFSA plans to carry out a broader review of the policy framework in 2024.

Although crypto tokens and investment tokens both form an integral part of the DFSA's broader digital assets regime in DIFC, they are both regulated under separate frameworks (the investment tokens framework is discussed above). The crypto tokens regime went live in November 2022 following the DFSA's publication of its Consultation Paper No. 143 on the Regulation of Crypto Tokens (CP143) in March 2022 and the subsequent release of its Feedback Statement on the CP123 in October 2022. The crypto tokens regime is very comprehensive and regulates a wider scope of cryptoassets compared to the investment tokens regime, covering not only the definition and promotion of crypto tokens but also establishing clear rules for other categories of tokens including 'excluded tokens' and 'prohibited tokens', as well covering other regulatory requirements in this regard such as market abuse, Islamic finance and token custody.

Read this article on Lexology

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Following a public consultation, in June 2018 the Financial Services Regulatory Authority (FSRA) issued its framework for the regulation of spot cryptoasset activities, including those undertaken by exchanges, custodians and other intermediaries in the ADGM. Specifically, the FSRA introduced the new regulated activity of 'operating a crypto asset business' that covers, among other things, the arranging, buying, selling, custody provision, marketing and advising on the merits of the buying or selling of 'accepted cryptoassets'. The regime also included a regulatory framework for the operation of a 'cryptoassets exchange' and a 'cryptoasset custodian'.

On 14 May 2019, the FSRA issued its updated guidance addressing, among other things:

- Stablecoins and fiat tokens: stablecoins that are fully backed by fiat currencies (fiat tokens) will be treated as a form of digital representation of money. Where used as a payment instrument for the purposes of money transmission as defined under the ADGM's Financial Services and Markets Regulations 2015 (FSMR), the activity will be licensed and regulated as 'providing money services'.
- Custody: further clarity on the types of cryptoasset custody activities that can be undertaken and setting out FSRA expectations in terms of custody governance and operations.
- Technology governance: further enhancements and clarifications are introduced, including in relation to changes in the underlying protocol of a cryptoasset that results in a fork (coding change), and the associated governance and control expectations for cryptoasset exchanges and licence holders.
- FSRA Anti-Money Laundering and Sanctions Rules and Guidance: as the Anti-Money Laundering Rulebook applies in full to the regulated activity of cryptoasset operators or holders, the guidance has been updated with the latest local and global changes and provides further clarity on the use of new regulatory and surveillance technologies in this area.

As part of its ongoing commitment to regularly update and improve its crypto-regulatory framework based on global developments, the FSRA updated its virtual asset regulatory framework in February 2020.

Among other things, the key amendments include:

- changing the definition of 'cryptoasset' to 'virtual asset' (to align the terminology with that of the Financial Action Task Force); and
- moving the applicable regulations and rules from the bespoke category of 'operating a crypto asset business' to the respective underlying regulated activities (eg, providing custody, operating a multilateral trading facility and dealing in investments). This is to better reflect the nature of the underlying activities in relation to virtual assets.

In October 2019, the SCA issued draft legislation – the Regulation for Issuing and Offering Crypto Assets – that, when implemented, will directly regulate cryptoassets in the UAE,

including crypto exchanges. In 2020, the SCA issued Board Decision No. 23/RM 2020, which applies to exchanges based on cryptoassets.

In June 2021, the UAE Central Bank issued the Retail Payment Services and Card Schemes Regulation. This regulates payment service providers and requires firms providing payment token services in onshore UAE (excluding the DIFC and the ADGM) to obtain a licence from the UAE Central Bank. The definition of payment token is narrow, however, only covering fiat-backed stablecoins.

The DFSA's regulatory framework is currently limited to investment tokens, which can be categorised as security tokens or derivative tokens. These provisions will apply to parties that market, issue, trade or hold investment tokens in or from the DIFC or authorised firms that intend to undertake financial services relating to investment tokens. However, following CP143, the DFSA is expected to introduce a broader regulatory regime encompassing any token that can be used as a 'medium of exchange or for payment or investment purposes' other than utility tokens, NFTs and central bank digital currencies. Investment tokens will continue to be regulated by the provisions currently in place. The new regulations may also require firms to obtain DFSA approval for each crypto token they intend to use for regulated activities (eg, marketing, issuing or trading).

The Dubai Virtual Assets Law applies onshore in the Emirate of Dubai (excluding the DIFC) and covers both 'virtual assets' (digital representations of value) and 'virtual tokens' (digital representations of sets of rights that can be offered and traded through digital platforms). It also requires platforms to obtain licences from VARA to provide services of exchange (namely, exchange between virtual assets and fiat currencies or between one or more forms of virtual assets) and services relating to the offering of or trading in virtual tokens. While VARA licence holders are currently only permitted to provide services to institutional investors, the regulator is expected to expand the scope of its licences to include retail investor activities before the end of 2022.

As a general point, in February 2023, the UAE Central Bank issued a press release announcing the launch of the Financial Infrastructure Transformation (FIT) Programme to promote the digital transformation across the financial services sector in the region. The FIT Programme is set to be integrated by 2026 and is divided into nine key pillars, one being central bank digital currency (CBDC). This initiative is part of the first stage of the implementation of the programme, which aims to develop a number of digital payment infrastructures and services such as the issuance of CBDCs for cross-border and domestic uses. According to the press release, by doing this the UAE Central Bank aims to improve the inefficiencies of domestic payments.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

The Financial Services Regulatory Authority (FSRA) has issued a regulatory framework for digital investment managers (robo-advisers) operating in the Abu Dhabi Global Market (ADGM). To supplement this, the FSRA has also released guidance to illustrate how its regulatory framework applies to robo-advisers in the ADGM. In particular, the guidance outlines:

- the regulatory permissions that may be required to provide digital investments services in or from the ADGM; and
- how the FSRA will apply its authorisation criteria in key existing areas of technology governance, suitability and disclosure, and newer areas such as algorithm governance.

In addition, certain sector-focused regulations, particularly data protection laws (as set out in more detail below) do cover topics such as automated decision-making and profiling, which, by extension, are likely to govern the activities of certain artificial intelligence (AI) systems and machine learning (tools that are commonly used in the fintech space) from a data privacy perspective. More recently, in April 2023, the Dubai International Financial Centre (DIFC) issued Consultation Paper No. 2 of 2023, which includes proposals to amend DIFC's existing Data Protection Regulations 2020. Such updates include obligations on controllers and processors who process personal data through the use of digital enablement technology systems (including AI and autonomous and automated systems).

It should also be noted that in 2019, Smart Dubai introduced the 'ethical AI toolkit' that lays out non-binding guidelines and standards, for the providers of AI services and systems, in respect of the ethical and responsible use of AI.

Otherwise, there are currently no formal rules or regulations governing the use of artificial intelligence or automated investment advice (namely, robo-advisory services) in the DIFC or onshore UAE. Those conducting these automated investment activities will need to ensure that they are authorised to provide investment advice, irrespective of the method of delivery.

The Dubai Financial Services Authority's (DFSA) Innovation Testing Licence regime has been used to issue licences relevant to automated investment advisory services. In these cases, there are bespoke disclosures, reporting conditions and monitored progress in line with an agreed 'regulatory test plan'. Firms intending to provide robo-advisory services have also been accepted into the ADGM's Regulatory Laboratory (which provides a controlled environment for fintech participants to develop and test innovative fintech solutions).

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Under the Dubai International Financial Centre and Abu Dhabi Global Market frameworks, there are detailed provisions relating to changes of control, including where notifications need to be made with the Dubai Financial Services Authority (DFSA) or the Financial Services Regulatory Authority respectively, or where their prior approval needs to be obtained. In both cases, these are contained in the general modules of the respective regulator's rulebook. Similar, although less detailed, provisions exist within the regulatory frameworks relevant to the UAE Central Bank and the UAE Securities and Commodities Authority.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

In March 2021, the Securities and Commodities Authority (SCA) introduced the Board of Directors Decision No. 23/RM of 2020 Concerning the Regulation of Cryptoassets and Administrative Decision No. 11 of 2021 Concerning Guidance for Cryptoasset Regulations. It is now a specific requirement for persons conducting financial activities in respect of cryptoassets to apply the Financial Action Task Force's guidance and recommendations in respect of the mitigation of anti-money laundering (AML) risks for virtual assets and virtual asset services providers (VASPs), in addition to any standards issued by the UAE Central Bank in respect of Financial Action Task Force guidance. The SCA's regulations on virtual assets, which entered into force in 2020, have also introduced financial crime controls, including AML protections and market abuse provisions, to all market participants. The regulations permit regular enhancements to the standards and requirements in line with global developments.

In 2021, the UAE Central Bank issued, among others, the updated Guidelines for Financial Institutions on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations, which is applicable to financial institutions. The guidelines provide additional clarity on the preferred risk-based approach and standards expected of a financial institution's AML and sanctions programmes. In conjunction with this, in May 2023, the UAE Central Bank issued further guidance to assist licensed financial institutions identify the money laundering risks and vulnerabilities related to virtual assets and VASPs, and to assist such institutions comply with their legal obligations in this regard. However, these guidelines are not intended to have force of law and are to be read in conjunction with the relevant laws, cabinet decisions, regulations and regulatory rulings in force.

Outside the cryptoasset regulations, the UAE's AML provisions apply directly to financial institutions and designated businesses and professions. While the UAE's anti-bribery and

corruption (ABAC) provisions apply to all individuals and entities in the UAE, there are currently no positive requirements in relation to ABAC; however, it is a positive obligation to notify the authorities if you become aware of any criminal offence.

In the Dubai International Financial Centre (DIFC), under article 71(1) of the DIFC Regulatory Law No. 1 of 2004, the DIFC regime requires compliance with the federal regime. The federal legislation governing money laundering and terrorist financing is also applicable in the DIFC. The Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module to the Dubai Financial Services Authority (DFSA) Rulebook applies to entities in respect of their activities carried on in or from the DIFC. The procedures that must be put in place include applying a risk-based approach that is objective and proportionate to the risks, based on reasonable grounds, properly documented and reviewed and updated at appropriate intervals. Effective AML systems and controls must also be established and maintained to prevent opportunities for money laundering. A risk-based assessment must be undertaken for every customer to assign the customer a risk rating proportionate to the customer's money laundering risks. Customer due diligence must be undertaken to verify the identity of the customer and the beneficial owner and understand the source of funds. This should be ongoing by monitoring transactions and complex and unusual transactions. A money laundering reporting officer must be appointed with responsibility for implementing and overseeing compliance; the officer must have an appropriate level of seniority and independence to act in the role and be resident in the UAE.

Similar to the DIFC, the federal legislation governing money laundering and terrorist financing also applies within the Abu Dhabi Global Market (ADGM). The ADGM's AML rules are contained in the Anti-Money Laundering and Sanctions Rules and Guidance Module to the Financial Services Regulatory Authority Rulebook (the ADGM AML Module). According to the ADGM AML Module, an entity must have policies, procedures, systems and controls that ensure compliance with the federal law, enable suspicious customers and transactions to be detected and reported, ensure the entity can provide an appropriate audit of a transaction trail, and ensure compliance with any other obligations as contained in the ADGM AML Module. The DIFC's AML rules are contained in the DFSA's Anti-Money Laundering, Counter Terrorist Financing and Sanctions Module.

In March 2022, the UAE was added by the Financial Action Task Force, the global financial crime watchdog, to the Grey List, a list of counties that are under increased monitoring because of deficiencies in their AML and countering the financing of terrorist regimes. The UAE has committed to implementing the recommendations of the Internal Cooperation Review Group's Action Plan to remove itself from the Grey List and improve its regimes.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no guidance specifically targeted at fintech companies. The regulatory guidance on financial crime is contained in the DFSA AML rules, the ADGM AML rules and the applicable federal laws and regulations. Federal legislation targeting financial criminal activities applies equally to individuals and companies operating or present in the commercial-free zones, financial fee zones and throughout all Emirates of the UAE.

Read this article on Lexology

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The Federal Decree-Law No. 45/2021 On the Protection of Personal Data (the UAE PDP Law) has been issued but will only be fully enforceable six months after the issuance of the corresponding executive regulations (the PDPL Regulations). The PDPL Regulations, which will contain further details and conditions of the UAE PDP Law, have yet to be issued.

Until then, the UAE still does not have a specific, enforceable standalone data protection law. Instead, various general and sector-specific laws and regulations govern aspects of the processing of personal data in the UAE. For example:

- the UAE Constitution provides for a right to freedom and secrecy of communications;
- the Penal Code and Cybercrime Law provide for a range of criminal offences prohibiting the disclosure or publication of private information and the interception of personal communications;
- the Civil Code and Labour Law set out certain obligations on employers when dealing with employee information;
- another law governs the collection, processing and disclosure of credit-related information; and
- telecoms operators are subject to special regulations regarding the protection of subscriber information.

In addition, certain health-related laws such as the Federal Decree-Law No. 2/2019 Concerning the Use of Information and Communication Technology in Health Fields cover certain requirements in respect of the processing, security, retention and transfer of health data – which fintech businesses providing healthcare-related products and services may need to consider.

The Abu Dhabi Global Market (ADGM) and the Dubai International Financial Centre (DIFC) have each introduced standalone laws governing the processing of personal data by organisations operating in their respective zones.

The DIFC's much anticipated new and refreshed Data Protection Law, DIFC Law No. 5 of 2020 was enacted on 1 June 2020 and became enforceable from 1 October 2020. The data protection law is enforced by the Commissioner of Data Protection and is also supplemented by the Data Protection Regulations 2020. In March 2022, the DIFC introduced the DIFC Laws Amendment Law, DIFC Law No. 2 of 2022, which includes amendments to several DIFC laws, including the data protection law. Such changes include clarification on the judicial redress process, increased accountability obligations on controllers and processors and the granting of additional powers to the Commissioner of Data Protection, as well as introducing a new monetary penalty. Further key amendments to DIFC's existing Data Protection Regulations 2020 have also been proposed through the issuance of Consultation Paper No. 2 of 2023 in April 2023. Subject to any further refinements, the updated Data Protection Regulations 2020 are expected to be rolled out in due course.

Read this article on Lexology

On 11 February 2021, the ADGM enacted the Data Protection Regulations 2021, which replaced the Data Protection Regulations 2015. The 2021 regulations, which formally came into effect on 14 February 2022, have been modelled on international best practice and, in particular, the European Union's General Data Protection Regulation but have been adapted to cater to the needs of the ADGM. A key feature of the new regulations is the establishment of an independent Office of Data Protection headed by a Commissioner of Data Protection.

In February 2022, the DIFC granted adequacy recognition to Singapore, South Korea and other countries that are part of the Asia Pacific Economic Cooperation Cross-Border Privacy Rules, for the purpose of cross-border personal data transfers with the DIFC.

In December 2022, the DIFC chief executive officer and the Commissioner of Data Protection issued a joint statement with the UK Minister of State for Media, Data and Digital Infrastructure regarding positive progress on the building of a 'data bridge' to promote trusted and secure data flows between the two jurisdictions. Similar announcements were also made by ADGM.

The DIFC and ADGM laws require that personal data is processed in a manner that is fair, lawful and secure.

Fintech-specific rules and regulations

The UAE Central Bank's Stored Value Facilities Regulation (the SVF Regulation) requires licensees to maintain adequate systems and policies related to data protection to ensure the protection of information from unauthorised access, ensure encryption of sensitive data, retrieval access controls must also be enforced to ensure confidentiality and integrity of the databases. The SVF Regulation also requires licences to implement an information retention and disposal policy to limit the data storage amount and retention time. In addition, the Retail Payment Systems Regulation (the RPS Regulation) also imposes data protection, security and integrity obligations on RPS licensees.

The UAE Central Bank has also issued the Consumer Protection Regulation (Circular No. 8/2020), which regulates the way financial institutions have to deal with consumer data in the UAE. A few of the changes introduced include the requirement to report significant data breaches, the establishment of a department dedicated to managing consumer data protection, the need to have security measures to protect consumer data and a limit on the amount of data collected from consumers (namely, data is to be used and stored for the duration necessary to provide financial services).

More recently, the Virtual Assets and Related Activities Regulations 2023 (the Virtual Assets Regulations) would require applicable fintech businesses (operating as virtual asset service providers (VASPs) under the regulations) to comply with activity-specific rulebooks (in addition to the five Virtual Assets Regulatory Authority (VARA) compulsory rulebooks) relating to their provision of the relevant virtual asset activities. Most notably, VARA's compulsory rulebook on technology and information requires VASPs to comply with applicable UAE data protection and privacy laws – including the requirement to appoint a data protection officer, establish an organisational function responsible for the management and protection of personal data, data breach notification requirements, as well as other controls and procedures.

Read this article on Lexology

Anonymisation and aggregation of personal data

There are no specific legal requirements or regulatory guidance in the UAE dealing with the anonymisation or aggregation of personal data used for commercial gain. This, and the absence of a specific data protection law in the UAE (outside the financial free zones) (subject to the UAE PDP Law becoming enforceable), has resulted in a wider scope for the commercial exploitation of data for commercial purposes in the UAE.

The definitions of 'personal data' in the ADGM and DIFC data protection laws each require the individual to whom the data relates to being identifiable. The guidance published by the DIFC Commissioner of Data Protection suggests that, as data that is stripped of all personal identifiers will no longer relate to an identifiable individual, the DIFC data protection law will no longer apply.

The guidance cautions that complete anonymisation may be difficult to achieve in practice, as data will still be protected if it is possible to identify an individual indirectly using the data. The guidance also reminds organisations that the act of anonymisation is itself an activity that must be conducted in compliance with the DIFC data protection law. The guidance published in respect of the ADGM data protection regime does not provide further comment on the anonymisation or aggregation of personal data.

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

Fintech businesses must comply with the UAE Federal Decree-Law No. 34/2021 Concerning the Fight Against Rumours and Cybercrime (the Cyber Crimes Law), the provisions of which broadly relate to IT security, state security and political stability, morality and proper conduct and financial and commercial issues arising from the use of the internet or IT infrastructure. It also addresses cybercrimes that are prepared, planned, directed, supervised or financed in the UAE. The Cyber Crimes Law has extraterritorial effect.

Various ongoing cybersecurity obligations apply to applicants of payment services licenses from the UAE Central Bank in the Payment Services Regulations.

For the purposes of the Virtual Assets Regulations, VARA's compulsory rulebook on technology and information requires VASPs to create and implement, among other things, a cybersecurity policy containing mandatory terms and security controls as set out in that rulebook.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

The UAE Central Bank has issued Central Bank Circular No. 14/2021 (the Outsourcing Regulations) to adopt minimum acceptable risk management standards for outsourcing arrangements, particularly when international service providers are engaged. With the new Outsourcing Regulations, and the accompanying Outsourcing Standards for Banks 14/2021 (the Outsourcing Standards), the UAE Central Bank makes explicit its objective to guarantee the soundness of UAE banks and improve financial stability in the banking sector. The Outsourcing Regulations impose obligations on the internal audit and operational risk functions of UAE banks and are expected to implement various new policies, procedures and controls. In particular, banks will need to create a comprehensive risk management framework that takes into account the additional risks that arise when business activities are outsourced.

Further, new minimum standards for outsourcing agreements have been introduced including certain contractual terms that have become standard inclusions across the market, for example, the requirement that banks retain full ownership of the data they share with outsourcing service providers. The Outsourcing Regulations also provide that data required to conduct the core activities of the bank must be maintained and stored within the UAE and any customers' confidential data must not be shared outside the UAE without the UAE Central Bank's approval and consent of their customers.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

There are regulations that set parameters around the use of cloud computing in the context of outsourcing, which includes those within the financial services industry.

Organisations carrying out functions that are regulated by the Dubai Financial Services Authority (in Dubai International Financial Centre) or the Financial Services Regulatory Authority (FSRA) (in the Abu Dhabi Global Market) have specific obligations in relation to material outsourcings, which in practice will include many cases of the use of cloud computing services. In respect of each material outsourcing, the organisation must implement policies and risk management programmes, enter into an appropriate contract with the service provider incorporating certain minimum terms, and notify the relevant regulator of the outsourcing arrangement. The Stored Value Facilities Regulation allows licensed businesses to outsource processes to third-party service providers, including independent third parties or companies within the licensee's group, subject to approval from the UAE Central Bank. A separate section of rules governing outsourcing applies when an outsourcing is considered for an operational function or activity, although no specific distinction or guidance is given in relation to cloud computing solutions.

Read this article on Lexology

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Original computer programs and related software applications are protected by copyright as literary works. Databases underlying software programs can also attract copyright protection. Copyright arises automatically as soon as the relevant literary work is created, so when a computer program is recorded, software lines are coded or a database is created. There is no requirement to register these rights to be able to have them recognised or enforce them against a third party in the UAE.

If the software code has been kept confidential, it may also be protected as confidential information and unauthorised disclosure can attract criminal sanctions. No registration is required.

As computer programs are not specifically excluded from patentability under UAE legislation, so long as registration formalities are followed, it is possible in principle to obtain patent protection for software-implemented inventions and business methods. It is likely to be more difficult, however, for these inventions to meet the criteria of novelty, inventiveness and industrial applicability as required by UAE legislation.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

The Federal Law No. 38 of 2021 concerning Copyright and Neighbouring Rights (the New Copyright Law) replaces the old Federal Law No. 7 of 2002 as of January 2022 (the Old Copyright Law). The New Copyright Law now reverses the position under the Old Copyright Law by confirming the 'work for hire' doctrine. Article 28 of the new Copyright Law states that any intellectual property created during the course of employment belongs to the employer and not the employee. However, any copyright made by an employee unrelated to the business of the employer that does not use the employer's resources will remain with the employee.

In the context of patents, provided that an employee's role includes inventive activities, inventions created by an employee in the course of an employment contract are automatically owned by the employer, unless otherwise agreed. Different rules apply if the employee's role does not include inventive activities. In these cases, the employer may exercise an option to take ownership of the invention within four months of becoming aware of the invention and the employee is entitled to receive fair compensation.

Similar to the New Copyright Law, under Dubai International Financial Centre (DIFC) Law No. 4 of 2019 on Intellectual Property, the employer has automatic ownership rights over works created by employees when produced within the scope of employment or while using

the employer's resources, unless otherwise agreed by them. The same position applies to patents. The law also regulates ownership rights over works created by contractors or consultants.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Joint owners of a copyright-protected work in which it is not possible to separate the contributions of each owner cannot exercise their rights to use, license or assign the work individually, unless otherwise agreed in writing (article 26 of the New Copyright Law).

Where multiple authors contribute different kinds of art to a single work, they may each exploit their individual contributions provided that this does not damage the exploitation of the joint work. The legal position is less clear in relation to works that include contributions of the same kind of art from multiple contributors.

A joint owner of a patented invention may exploit or assign his or her rights independently of the other patentees. However, joint patentees may only license the exploitation of the patent jointly with the other patentees.

Under DIFC Law No. 4 of 2019 on Intellectual Property, rights over an invention created by two or more persons, will be shared equally between them unless otherwise agreed in writing.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

The UAE legislation dealing with patents and industrial designs also includes specific protection for trade secrets and know-how. Employees have specific statutory duties to keep the commercial and industrial secrets of their employers confidential and may be criminally liable in cases of unlawful use or disclosure of information. Trade secrets and confidential information more broadly are commonly protected by way of contractual obligations.

Court proceedings in the UAE are not held in public and there is therefore less of a concern about maintaining the confidentiality of trade secrets in this context.

DIFC Law No. 4 of 2019 on Intellectual Property provides protection to trade secrets if obtained by improper means. However, it may be possible to uncover trade secrets through legitimate means.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brands can be protected as registered trademarks in the UAE. An application for registration and other formalities must be pursued to obtain protection. A law recognising a unified trademark regime for Gulf Cooperation Council countries has been decreed in the UAE but has not yet entered into force.

The UAE trademark database can be used to identify registered trademark rights and, therefore, help ensure that a fintech business does not infringe on existing brands. The database is not available to the public but the law provides for a right to obtain a certified extract of the contents of a register upon payment of a fee. Applicants must pay a separate fee to search each class for existing trademark rights.

It is highly advisable for new businesses, perhaps using the services of specialist trademark attorneys, to check whether the database enquiry results indicate earlier registrations that are identical or similar to their proposed brand names and marks. It may also be advisable to conduct internet searches for any unregistered trademark rights that may prevent the use of the proposed mark.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

Remedies available to individuals or companies include:

- precautionary measures, including requirements to cease the use of an infringing item;
- confiscation or destruction of infringing items;
- damages; and
- publication orders.

The UAE legislation dealing with intellectual property rights, including in respect of patents, designs, trademarks and copyright, provides for criminal liability in various cases of infringement.

DIFC Law No. 4 of 2019 on Intellectual Property introduces penalties for infringement of intellectual property rights. The DIFC courts can also issue injunction orders and award damages resulting from the violation of intellectual property law.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

Since the enactment of Federal Law No. 12 of 2012, the UAE has had a standalone, federally applicable competition law that covers anticompetitive agreements, abuse of dominance and merger control; however, the law also has a list of sectors that are entirely excluded from its scope. One of these wholly excluded sectors is the financial sector. The list of excluded sectors and other important aspects of the competition regime in the UAE is within the discretion of the Ministry of Economy, and fintech businesses in the UAE will need to consider their specific competition law issues to assess their exposure. Looking ahead, there is expected to be increased consolidation in the banking sector and an expectation of greater collaboration, information-sharing and other horizontal arrangements, all of which could give rise to competition law risks in the UAE.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

There are no special incentives. However, onshore UAE, the Dubai International Financial Centre and the Abu Dhabi Global Market are all currently low or zero-tax jurisdictions.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

There are no relevant new or proposed tax laws or guidance.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

Once an employee enters the UAE on an entry permit, the employer must make an application for a residence visa to the immigration authorities. Before the visa is granted, the employee must pass a medical examination. These requirements must be satisfied within 60 days of the employee's entry into the UAE on the entry permit. Residence visas are typically

valid for two years outside the free zones and three years for employees within a free zone. The total cost of the residence visa and the required permits depends on the nature of the company's activity and whether the employee is hired within or outside the UAE. The cost outside the free zones ranges from US$400 to US$1,200. Free zone costs can differ.

Both financial free zones in the UAE offer start-up-specific licences that, if obtained, provide for the recruitment of skilled staff from outside of the UAE. In 2018, the Abu Dhabi Global Market (ADGM) introduced the ADGM Tech Start-up Commercial Licence, under which it is possible to secure up to four UAE residence visas. In the Dubai International Financial Centre (DIFC), the DIFC FinTech Commercial Licence enables fintech start-ups to apply for residence visas for their staff, the number of which is dependent on office space (generally one visa per 80 square feet).

Investor visas are available to shareholders and proprietors.

The UAE government announced the UAE Strategy for Talent Attraction and Retention, an initiative aimed at enhancing the country's attractiveness to foreign investments and talents. The strategy aims to position the UAE among the top 10 countries in the global talent competitiveness indices, ensure the availability of talented workforce all across strategic sectors and cement the UAE's image as an ideal destination for living and working.

The UAE also announced its remote working visas for overseas professionals and the Dubai virtual working programme for a period of one year to attract talent and expertise from all over the world.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

No updates at this time.

Raza Rizvi raza.rizvi@simmons-simmons.com
Muneer Khan muneer.khan@simmons-simmons.com

Office 17-04 Level 17 ICD Brookfield Place, Dubai International Financial Centre, PO Box 506688, Dubai, United Arab Emirates
Tel: +971 4 709 6600
www.simmons-simmons.com

Read more from this firm on Lexology

Read this article on Lexology

United Kingdom

George Morris, Oli Ward, Sophie Sheldon, Olly Jones and Gordon Ritchie*
Simmons & Simmons

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 662
General innovation climate 662
Government and regulatory support 664

FINANCIAL REGULATION 665
Regulatory bodies 665
Regulated activities 666
Consumer lending 667
Secondary market loan trading 669
Collective investment schemes 669
Alternative investment funds 670
Peer-to-peer and marketplace lending 670
Crowdfunding 672
Invoice trading 672
Payment services 673
Open banking 675
Robo-advice 675
Insurance products 676
Credit references 676

CROSS-BORDER REGULATION 677
Passporting 677
Requirement for a local presence 677

SALES AND MARKETING 678
Restrictions 678

CRYPTOASSETS AND TOKENS 680
Distributed ledger technology 680
Cryptoassets 681
Token issuance 683

ARTIFICIAL INTELLIGENCE 684
Artificial intelligence 684

CHANGE OF CONTROL 686
Notification and consent 686

Read this article on Lexology

FINANCIAL CRIME	**687**
Anti-bribery and anti-money laundering procedures	687
Guidance	689
DATA PROTECTION AND CYBERSECURITY	**689**
Data protection	689
Cybersecurity	691
OUTSOURCING AND CLOUD COMPUTING	**692**
Outsourcing	692
Cloud computing	694
INTELLECTUAL PROPERTY RIGHTS	**695**
IP protection for software	695
IP developed by employees and contractors	695
Joint ownership	696
Trade secrets	696
Branding	697
Remedies for infringement of IP	697
COMPETITION	**698**
Sector-specific issues	698
TAX	**700**
Incentives	700
Increased tax burden	701
IMMIGRATION	**702**
Sector-specific schemes	702
UPDATE AND TRENDS	**703**
Current developments	703

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

The United Kingdom has been at the forefront of innovation in technology and finance for many years. Despite the disruption caused by the UK's departure from the European Union and the effects of the covid-19 pandemic, this remains the case today. As the worlds of technology and finance become increasingly linked, London, in particular, has the unique advantage of being the national centre of government and finance and having many world-class universities nearby. Fintech businesses also benefit from the UK's time zone, language and legal system. Unlike the European Union and the United States, the United Kingdom has a small number of regulators, with central government setting the overall framework and able to take decisive action that allows legislators and regulators to react to the fast-moving technology sector.

Read this article on Lexology

The United Kingdom still dominates the European market in terms of fintech investment and was second only to the United States in terms of level of capital raised in 2022.

According to data from the UK's fintech trade association, Innovate Finance, while the global fintech market experienced a 30 per cent contraction in 2022, the United Kingdom has demonstrated its resilience as a top destination for fintech. In 2022 fintech companies in the United Kingdom attracted US$12.5 billion in investment capital, confirming the country's leading position in European fintech rankings, recording greater venture capital investment than the combined total of the subsequent 13 European markets.

Perhaps mindful of the potential effect of Brexit, the government has been keen to promote the United Kingdom as a fintech-friendly jurisdiction. As part of this policy objective, in July 2020, the UK Chancellor asked Ron Kalifa OBE to conduct an independent review to identify priority areas to support the UK's fintech sector. The resulting report, the Kalifa Review, was published in February 2021 and provided a five-point plan to allow the United Kingdom to extend its competitive advantage over other fintech hubs by creating a framework for innovation and supporting UK fintech firms to scale up. Recommendations included:

- amendments to UK listing rules to make the United Kingdom a more attractive location for initial public offerings;
- improvements to tech visas to attract global talent and boost the fintech workforce;
- creation of a regulatory fintech scalebox to provide additional support to growth-stage fintechs; and
- establishment of a centre for finance, innovation, and technology, to strengthen national coordination across the fintech ecosystem to boost growth.

We are starting to see progress on the recommendations, particularly around policy and regulation initiatives with the government's focus on fintech further endorsed in April 2023 by the Economic Secretary to the Treasury, Andrew Griggith MP. In his speech to the Innovate Finance Global Summit during UK Fintech Week, Griggith reaffirmed the government's desire to make the United Kingdom a pro-innovation jurisdiction. He reiterated the crucial role played by fintech plays in the economy and, as evidence of this, he mentioned recent government initiatives.

Griggith mentioned the new HM Treasury consultation on the UK regulatory approach to crypto assets and stablecoins published in February 2023, highlighting how the UK government 'pro-actively support the use of DLT and tokenisation'. Griggith also discussed the upcoming Financial Market Infrastructure Sandbox, 'which will help industry adopt and scale digital solutions that could radically change the way markets operate'.

In addition, he also highlighted the government's efforts in introducing an agile regulatory framework for payments and e-money reflected in the submission to the Payment Services Call for Evidence, with the aim of fostering an internationally competitive payment sector.

The UK government's efforts to support the fintech industry is also evidenced by the launch in February 2023 of the new Centre for Finance, Innovation, and Technology (CFIT). This initiative is backed by £5.5 million of HM Treasury and City of London Corporation funding and aims to bring together indstry players – entrepreneurs, policymakers, investors and

Read this article on Lexology

academics – into coalitions to address some of the trickiest challenges facing the sector. Griggith announced that this year the CFIT's first coalition will focus on open finance.

More broadly, the UK government has announced a significant package of 30 regulatory and tax reforms (the Edinburgh Reforms). The proposed reforms represent a commitment from the government to build on the UK's position following Brexit and, of particular interest, include proposals on modernising the regulatory frameworks concerning the remit of regulators, fund management, payments and payment accounts, e-money, and the provision of regulated credit.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

In addition to the overall policy support articulated by the government described in relation to the UK's regulatory bodies have established numerous initiatives and services to support fintech companies over the years.

In particular, the Financial Conduct Authority (FCA) started Project Innovate in 2014 to encourage innovation and promote competition. The support offered by Project Innovate has evolved over time, which is outlined in the FCA Innovation Hub. Currently, the FCA provides the following services:

- the Regulatory Sandbox, which allows businesses to test innovative propositions in the market with real consumers. Historically, the FCA allowed firms to participate in a series of cohorts that were open for applications in specific windows, but since 2021 the Sandbox has been open for applications at any time. This approach was also encouraged in the Kalifa Review of UK Fintech, thanks to which firms can now access the FCA testing services 'at any point throughout the year, at the right point in their development lifecycle, at a time that works best for them';
- the Innovation Pathways, which helps innovative firms to understand and navigate the UK's regulatory regime. Support via Innovation Pathways is available to both new and established businesses and includes the provision of a dedicated FCA case manager to provide guidance on whether new business models require authorisation and how to apply for authorisation or a variation of existing permissions. Innovation Pathways combines the support historically provided by the FCA through its Direct Support programme and the Advice Unit, which provided feedback to firms developing automated advice and guidance models;
- the Digital Sandbox, which provides fintech companies with access to online tools and high-quality synthetic data to test and develop their propositions at the proof-of-concept stage. First piloted in 2020, the Digital Sandbox has shown that collaboration and access to data can stimulate beneficial innovation in the market. Following two successful pilots, the FCA confirmed that the FCA Digital Sandbox will become permanent during summer 2023;
- the Tech Challenges, designed to allow the FCA to play a more active part in driving innovation in an area where the FCA sees clear benefits to UK consumers and markets. To date, the FCA has run two Green FinTech Challenges to support firms developing innovative solutions to assist in the UK's transition to a net-zero economy;

Read this article on Lexology

- the TechSprints, also known as 'hackathons', which are events allowing the FCA to gather participants from across the financial services industry and beyond to develop technology-based ideas and discuss specific industry challenges. The two upcoming TechSprints in Q3 2023 are the Consumer Duty TechSprint, which will cover how open banking data can be leveraged and integrated into solutions to support the delivery of the New Consumer Duty and the Global Financial Innovation Network (GFIN) Greenwashing TechSprint, which will aim to develop a solution to help regulators addressing the risks of greenwashing in financial services across the globe. Previous TechSprints have covered diverse topics from model-driven machine executable regulatory reporting to women's economic empowerment; and
- industry events, such as roundtables and workshops, to help develop thinking on priority fintech areas and the ways in which practical and productive collaboration can take place at scale. An example of industry events are the Showcase Days for regtech firms to demonstrate their technology solutions to internal market experts within the FCA.

The FCA is also the founder member and chair of the GFIN. Formed in 2019, the GFIN is an international group of 70 financial regulators and related organisations that are committed to supporting financial innovation in the interest of consumers on an international basis. The GFIN was formed to provide a framework for cooperation between financial services regulators on innovation-related topics, sharing different experiences and approaches.

The Bank of England (BoE), is responsible for supervising financial firms such as banks, building societies, credit unions, major investment firms and insurers as well as financial market infrastructure providers and acting as settlement agent for payments systems and setting monetary policy in the United Kingdom. The BoE is also active in exploring how developments in fintech might both impact and support its mission to maintain monetary and financial stability. Among other initiatives, the BoE worked with the FCA to establish the Artificial Intelligence Public-Private Forum in 2020 to create further dialogue on artificial intelligence innovation between the public and private sectors. The BoE has also announced that it intends to work with the FCA to launch the new Financial Markets Infrastructure Sandbox in 2023 to support firms wishing to use new technology such as distributed ledger technology to provide infrastructure services to the financial markets. Separately, the BoE works directly with fintech businesses on proof of concept trials of technology that could be used by the BoE itself.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

The Financial Conduct Authority (FCA) is the financial services regulator for most regulated activities and services that a fintech would provide. The Prudential Regulation Authority (PRA) covers the prudential regulation of banks and insurers in the United Kingdom with the FCA regulating conduct matters (making banks and insurers dual-regulated entities). The FCA and the Payment Services Regulator (PSR) – which has a focus on competition and innovation – are the main regulators of payment systems and the financial institutions that participate in them.

Read this article on Lexology

Other relevant regulators that fintechs will need to be aware of are HM Revenue and Customs (HMRC) (the relevant regulator for money service businesses) and the Information Commissioner's Office (ICO).

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

There are a large number of activities (specified activities) that, when carried on in the United Kingdom by way of business in respect of specified kinds of investments, trigger licensing requirements in the United Kingdom. These are set out in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO). While it is not practical to list them all, the most common include:

- accepting deposits: this is mainly carried out by banks and building societies. An institution will accept a deposit where it lends the money it receives to others or uses it to finance its business;
- dealing in investments (as principal or agent): buying, selling, subscribing for or underwriting particular types of investments. In respect of dealing as principal, the specified investments are 'securities' and 'contractually based investments'. In respect of dealing as agent, the specified kinds of investments are 'securities' and 'relevant investments':
- arranging deals in investments (this is split into two activities and specified investments in respect of arranging include securities and relevant investments):
- advising on investments: advising a person in their capacity as an investor on the merits of buying, selling, subscribing for or underwriting a security or relevant investment or exercising any right conferred by that investment to buy, sell, subscribe for or underwrite such an investment;
- managing investments: managing assets belonging to another person, in circumstances involving the exercise of discretion, where the assets include any investment that is a security or contractually based investment;
- establishing, operating or winding up a collective investment scheme (CIS);
- certain lending activities: entering into a regulated mortgage contract or a regulated (consumer) credit agreement (or consumer hire agreement) as lender, together with various ancillary activities such as credit broking and debt collection;
- certain insurance activities: effecting a contract of insurance as principal and carrying out a contract of insurance as principal; and
- e-money: issuing e-money (as a bank).

Payment services and e-money activity have separate regulatory regimes under the Payment Services Regulations 2017 and Electronic Money Regulations 2011 respectively, both of which are derived from EU legislation.

The government has proposed introducing a new regulated activity relating to the custody, or arranging the custody, of a stablecoin as part of its approach to establishing a bespoke regulatory framework for this type of digital asset. If the firm provides or arranges custody for stablecoins and is recognised as 'systemic' then under the current proposals, the firm will be dual regulated by the FCA and the Bank of England (BoE). As part of the government's consultation process, it is proposing to apply and adapt existing frameworks for traditional finance custodians under for cryptoasset custody activities, making 'suitable modifications

to accommodate unique cryptoasset features', or putting in place new provisions where appropriate.

Consumer duty

Consumer duty is a key regulatory requirement, driven and regulated by the FCA, which is currently being implemented by firms, which will 'set higher expectations of firms driving a cultural reset that leads to enhanced confidence in financial markets and future gains from innovation'. The duty deals with information asymmetries and consumer cognitive and behavioural biases. It is applicable across multiple regulated activities and should be considered in a wide range of circumstances where firms have exposure to retail clients.

The consumer duty requires firms to review all UK products, services and communications aimed at retail customers across four outcomes (products and services, price and value, customer understanding, customer support). Firms need to design appropriate data-gathering and management information as the FCA expects a firm's board (or similar body) to consider whether it is acting to deliver good customer outcomes. The FCA has been clear that it is now a data-led regulator, and it is likely to look at this management information carefully as part of its assessment of whether firms have implemented the consumer duty in the way the FCA intended.

Firms that provide in-scope products or services are expected to have begun implementing the consumer duty ahead of the July 2023 implementation deadline (for products or services that are open to sale or renewal). The FCA has said that they will continue to support firms' embedding activities in the run-up to, and beyond, the July 2023 implementation deadline for new and existing products and services.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

The general position is that lending by way of business to consumers is regulated in the United Kingdom. The FCA is responsible for authorising and regulating consumer credit firms.

There are two categories of regulated lending: regulated credit agreements and mortgages.

Any person (A) who enters into an agreement with an individual (or a 'relevant recipient of credit', which includes a partnership consisting of two or three persons not all of whom are bodies corporate and an unincorporated body of persons that does not consist entirely of bodies corporate and is not a partnership) (B) under which A provides B with credit of any amount must be authorised by the FCA – unless an appropriate exemption applies.

Two of the most common exemptions are:

- where the amount of credit exceeds £25,000 and the credit agreement is entered into wholly or predominantly for business purposes; and
- where the borrower certifies that they are high-net-worth and the credit is more than £60,260.

Other complex exemptions are available that relate to, among other things, the total charge for the credit, the number of repayments to be made under the agreement and the nature of the lender.

If an exemption applies, the lender does not need to comply with the detailed legislative requirements that apply to regulated credit agreements contained in the Consumer Credit Act 1974 (CCA) (and secondary legislation made under it) and the FCA's Consumer Credit Sourcebook (CONC). Broadly, the CCA sets out the requirements lenders need to comply with in relation to the provision of information, documents and statements and the detailed requirements as to the form and content of the credit agreement itself.

HM Treasury (HMT) has proposed to regulate buy-now, pay-later (BNPL) credit under the RAO. The government's ambition is to lay legislation during 2023. The government is proposing legislative changes to article 60F(2) of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, which, currently, broadly exempts any borrower-lender-supplier agreement for fixed-sum credit where:

- the number of repayments is not more than 12;
- the repayments must be made over no more than 12 months; and
- no interest or fees are charged for the credit.

The government is narrowing this exemption considerably by removing from its scope:

- where the lender and the supplier are not the same person (that is, where the credit is provided by a person that is not the provider of the goods or services being financed); and
- where the lender purchases products from the supplier and resells them to the consumer on finance will become regulated, with agreements in these circumstances no longer being able to rely on the exemption and, therefore, likely requiring the lender to be regulated, unless an exemption applies.

In respect of any regulated credit agreement, if an exemption does not apply, the CONC chapter in the FCA Handbook sets out detailed rules that regulated consumer credit firms must comply with and covers areas such as the conduct of business, financial promotions, pre-contractual disclosure of information, responsible lending, post-contractual requirements, arrears, default and recovery, cancellation of credit agreements and agreements that are secured on land.

In addition to the CONC, authorised consumer credit firms must also comply with other applicable chapters of the FCA Handbook. Failing to comply with the requirements of the CCA may result in those agreements being unenforceable against borrowers and the FCA imposing financial penalties on the firm in question.

As part of the Edinburgh Reforms, the government has proposed a substantial modernisation of the regulated credit framework. This process is expected to take several years. Two of the key principles of the reforms will be proportionality and simplification, as well as some degree of harmonisation with other regulatory developments, such as the FCA's consumer duty. Some specific points under consultation include:

- changing or possibly abolishing the £25,000 minimum under the business lending exemption;
- reviewing and modernising information requirements in relation to regulated credit; and
- looking at how reform can encourage financial inclusion and remove barriers.

Where possible, the relevant regulatory rules will be moved into the FCA Handbook (from statute) and there may need to be some extension of FCA powers. The idea is that this will allow the rules to be flexible and to adapt rapidly to an evolving market.

Entering into a regulated mortgage contract is a regulated activity. Such contracts are loans where:

- the contract is one under which a person (lender) provides credit to an individual or trustee (borrower);
- the contract provides for the obligation of the borrower to repay to be secured by a mortgage on land in the United Kingdom; and
- at least 40 per cent of that land is, or is intended to be, used.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

Provided that the loan itself is being traded, and not the loan instrument (eg, an instrument creating or acknowledging indebtedness), then there are no restrictions on trading loans in the secondary market.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

Establishing, operating or winding up a CIS is a regulated activity in the United Kingdom for which firms must be authorised by the FCA.

The definition of a CIS is set out in section 235 of the Financial Services and Markets Act 2000 (FSMA). Broadly, a CIS is any arrangement with respect to property of any description, the purpose or effect of which is to enable the persons taking part in the arrangements to participate in or receive profits or income arising from the acquisition, holding, management or disposal of the property or sums paid out of such profits or income. The persons participating in the arrangements must not have day-to-day control over the management of the property. The arrangements must also have either or both of the following characteristics:

- the contributions of the participants and the profits or income out of which payments are to be made to them are pooled; or
- the property is managed as a whole by, or on behalf of, the operator of the scheme.

Whether a fintech company falls within the scope of this regime will depend on the nature of its business. For example, fintech companies that manage assets on a pooled basis on behalf of investors should consider carefully whether they may be operating a CIS. On the other hand, fintech companies that only provide advice or payment services may be less likely to operate a CIS. Certain cryptoassets or platforms that offer cryptoasset staking, in particular, may be exposed to the risk of being categorised as a CIS, but this analysis is fact-dependent. Fintech companies are advised to seek legal advice on this subject and to have regard to their other regulatory obligations.

The management of two forms of regulated collective investment schemes, undertakings for the collective investment in transferable securities and alternative investment funds, are also regulated activities. Peer-to-peer (P2P) or marketplace lenders or crowdfunding platforms are regulated separately under their own regimes.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

Managers of alternative investment funds are regulated in the United Kingdom under the EU Alternative Investment Fund Managers Directive, which has been implemented in the United Kingdom by the Alternative Investment Fund Managers Regulations 2013 and rules and guidance contained in the FCA Handbook. In a key divergence with the European Union, the United Kingdom has not implemented similar legislation to the EU's Cross-Border Distribution of Funds regime regarding the marketing of funds. Instead, certain elements are covered by the UK's financial promotion regime.

The FCA published a discussion paper this year on 'Updating and improving the UK regime for asset management', which raised questions for industry on opportunities to improve regulation of the asset management sector and introducing 'a more modern and tailored regime, better meeting the needs of UK markets and consumers'. As is usual for discussion papers, the discussion paper does not contain any firm proposals. A feedback statement on the FCA's findings is expected later in 2023.

Peer-to-peer and marketplace lending

9 | Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

P2P lending is a term that generally refers to loan-based crowdfunding. In the United Kingdom, the FCA regulates loan-based crowdfunding platforms.

Under article 36H of the RAO, operating an electronic system that enables the operator (A) to facilitate persons (B and C) becoming the lender and borrower under an article 36H agreement is a regulated activity (and a firm will require FCA authorisation) where the following conditions are met:

- the system operated by A is capable of determining which agreements should be made available to each of B and C;

- A (or someone acting on its behalf) undertakes to receive payments due under the article 36H agreement from C and make payments to B that are due under the agreement; and
- A (or someone acting on its behalf) takes steps to procure the payment of a debt under the article 36H agreement or exercises or enforces rights under the article 36H agreement on behalf of B.

An article 36H agreement is an agreement by which one person provides another with credit in relation to which:

- A does not provide the credit, assume the rights of a person who provided credit or receive credit; and
- either the lender is an individual or the borrower is an individual and the credit is less than £25,000, or the agreement is not entered into by the borrower wholly or predominantly for the purposes of a business carried on, or intended to be carried on, by the borrower.

In addition to falling within the definition of an article 36H agreement, a loan may also constitute a regulated credit agreement, unless an exemption applies and so a lender, through a platform authorised under article 36H, may also be required to have permission to enter into a regulated credit agreement as lender. Two of the most common exemptions are:

- where the amount of credit exceeds £25,000 and the credit agreement is entered into wholly or predominantly for business purposes; and
- where the borrower certifies that they are 'high-net-worth' and the credit is more than £60,260.

Other complex exemptions are available that relate to, among other things, the total charge for the credit, the number of repayments to be made under the agreement and the nature of the lender.

The rules governing P2P lending are found in the Conduct of Business Sourcebook and Senior Management Arrangements, Systems and Controls, and include:

- enhanced requirements for platform governance arrangements including in relation to credit risk assessment, risk management and fair valuation practices;
- strengthening rules on wind-down planning in the event of platform failure;
- setting out the minimum information that a platform should provide to investors; and
- introducing a requirement to monitor the investors that can use a platform, including that platforms assess investors' knowledge and experience of platform lending where no advice has been given to them. Firms are required to ensure that retail clients:

    - are certified or self-certified as 'sophisticated investors' or 'high-net-worth investors';
    - confirm before a promotion is made that they will receive regulated investment advice or investment management services from an authorised person; or
    - do not invest more than 10 per cent of their net investible assets in P2P agreements in the 12 months following certification.

P2P lending has recently been categorised as a 'restricted mass market investment' and so regulatory requirements have been placed on financial promotions in relation to such investments. Broadly these include a prescribed form of risk warning and requiring that the promotion does not include any form of incentive to invest.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

In the United Kingdom, reward-based crowdfunding (where people give money in return for a reward, service or product) and donation-based crowdfunding (where people give money to enterprises or organisations they wish to support) are not currently regulated in their own right.

Equity-based crowdfunding is where investors invest in shares in, typically, new businesses. Equity-based crowdfunding is not specifically regulated in the United Kingdom (in the same way as loan-based crowdfunding).

However, a firm operating an equity-based crowdfunding service must ensure that it is not carrying on any other regulated activity without permission. Examples of regulated activities that equity-based crowdfunding platforms may carry on (depending on the nature and structure of their business) include:

- establishing, operating or winding up a CIS;
- arranging deals in investments; and
- managing investments.

Additionally, equity-based crowdfunding platforms must not market to retail clients unless an appropriate exemption applies.

In the FCA's policy statement on P2P lending, investment-based crowdfunding platforms were also covered. Recent work has focused on restrictions on the types of clients these platforms can market to and how this is managed.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

Currently, there are no regulations relating specifically to invoice trading.

However, depending on how the business is structured, a firm that operates an invoice-trading platform may be carrying on regulated activities for which it must have permission, including:

- establishing, operating or winding up a CIS; and
- managing an alternative investment fund.

Payment services

12 | Are payment services regulated in your jurisdiction?

Payment services are regulated under the Payment Services Regulations 2017 (the Payment Services Regulations), which implement the EU second Payment Services Directive (PSD2) in the United Kingdom. Following, and relating to, Brexit the FCA published an updated version of its Approach Document setting out guidance for payment and e-money firms to reflect certain required amendments. Payment services include:

- services enabling cash to be placed on a payment account and all the operations required for operating a payment account;
- services enabling cash withdrawals from a payment account and all the operations required for operating a payment account;
- the execution of the following types of payment transaction:
    - direct debits, including one-off direct debits;
    - payment transactions executed through a payment card or a similar device; and
    - credit transfers, including standing orders; and
- the execution of the following types of payment transaction where the funds are covered by a credit line for the payment service user:
    - direct debits, including one-off direct debits;
    - payment transactions executed through a payment card or a similar device; and
    - credit transfers, including standing orders; and
- issuing payment instruments or acquiring payment transactions;
- money remittance;
- payment initiation services (initiating a payment order at the request of a payment service user with respect to an account held with another payment service provider); and
- account information services (online services that are intended to provide consolidated information on one or more payment accounts held by the payment service user with another one (or more) payment service provider).

The Payment Services Regulations broaden the scope of transactions governed by its provisions, narrow the scope of certain exclusions, amend the conduct of business requirements and introduce security requirements.

To provide payment services in the United Kingdom, a firm must fall within the definition of a 'payment service provider'(PSP). Payment service providers include authorised payment institutions, small payment institutions, credit institutions, e-money institutions, the post office, the BoE and government departments and local authorities.

A firm that provides payment services in or from the United Kingdom as a regular occupation or business activity (and is not exempt, or a bank) must apply for authorisation or registration as a payment institution.

E-money institutions are regulated under the Electronic Money Regulations 2011 (SI 2011/99). They must be authorised or registered to issue e-money and undertake certain payment services. The FCA's Approach Document provides useful guidance for e-money institutions alongside explanations of most requirements in the FCA Handbook.

The government has proposed significant reforms to the payments' framework as part of their consultation on the Payment Services Regulations under the Edinburgh Reforms. Key proposals include:

- the delegation of further payments regulation to the FCA;
- 'rationalising' the distinction between payment institutions and e-money institutions; and
- reviewing the regulatory regime for payment initiation service providers and account information service providers, and clarifying ambiguities in the Payment and E-Money Institution Special Administration Regime.

The PSR is also proceeding with plans to require the mandatory reimbursement of victims of authorised push payment fraud where payment is made over the Faster Payments Service. This will be subject to very limited exceptions and will apply to all PSPs (including indirect access providers). Firms will, generally, need to refund the consumer within 48 hours of the fraud being reported and costs will be expanded from sending firms, to now both sending and receiving PSPs, with an assumed but negotiable 50:50 split. The PSR is proposing some practical limits and will allow PSPs to:

- set a minimum threshold for reimbursement (of no more than £100);
- withhold an 'excess' (of no more than £35); and
- set a time limit for claims (of not less than 13 months).

The Financial Services and Markets Bill currently making its way through Parliament will allow the PSR to establish this system and it is expected that it should be fully implemented by the end of 2023.

The European Commission has launched several initiatives assessing the status of PSD2, including proposing changes to the regulatory oversight of certain delegated models, a simplification of the payments regime, and a central database to record sanctions across EU member states.

In respect of the card-acquiring market, the PSR has published a policy statement setting out its final decision on remedies for the card-acquiring market that covered:

- greater transparency to improve comparison; and
- greater engagement.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

Open banking has been operational since 2018 and has been driven by the United Kingdom's competition authority (the Competition and Markets Authority (CMA)) and the Open Banking Implementation Entity operating under the CMA's Retail Banking Market Investigation Order 2017, together with the implementation of PSD2.

Following its investigation into the retail and small and medium-sized enterprise (SME) banking sectors between 2013 and 2016, the CMA ordered a number of remedies to help promote greater competition in the retail and SME banking markets.

One of the core remedies ordered by the CMA requires the nine largest retail banks in Great Britain and Northern Ireland to develop and implement an open banking standard application programming interface (API) to give third parties access to information about their services, prices and service quality to improve competition, efficiency and stimulate innovation. The open APIs also allow retail and SME customers to share their own transaction data with trusted intermediaries, which can then offer advice tailored to the individual customer.

These measures are intended to make it easier for customers to identify the best products for their needs. Additionally, the Payment Services Regulations require banks to allow third-party payment service providers to initiate payments from their customers' accounts.

The UK open banking ecosystem is currently undergoing a process of expansion. While significant progress has been made in relation to open banking since its introduction, regulators have identified that more needs to be done to deliver the full benefits of open banking within retail banking markets, and beyond, and to maintain its international leadership. The Joint Regulatory Oversight Committee (JROC) has published its recommendations for the next phase of open banking in the United Kingdom. The recommendations also cover plans for the 'future entity' in charged with overseeing open banking and the underpinning principles of a future 'long-term regulatory framework', which the recommendations confirm the government is intending to legislate for. The JROC intends to monitor progress and will provide a first progress report (as well as the communication of its 'refined views' on the design of the future entity) in the fourth quarter of 2023. Full implementation is expected to take at least two years.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

There are no specific regulations to cover robo-advisers. The rules applying to investment advisers or arrangers and discretionary investment managers are technology-neutral and cover face-to-face as well as online or automated services. Therefore, a licence would generally be required, and robo-advisers would be subject to the usual conduct of business

requirements, for example, suitability assessments, disclosure of costs and charges, and marketing (which must be fair, clear and not misleading). The FCA provides some specific guidance for firms developing an automated advice or guidance proposition through a dedicated FCA Advice Unit. The FCA also evaluated the status of automated advice within the UK market in 2020, but with limited substantive action taken.

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Effecting or carrying out a contract of insurance, arranging contracts of insurance, or dealing in insurance as an agent are regulated activities and fintech companies that wish to do this must be regulated. Key regulation includes the retained EU law version of Regulation (EU) No. 1286/2014 on key information documents for packaged retail and insurance-based investment products and has been applied since the end of the Brexit transition period. Companies that wish to market insurance products must either be regulated, have their marketing material approved by a regulated firm or fall within an applicable exclusion. For example, exemptions may be available for communications to high-net-worth individuals, companies, sophisticated individuals and other investment professionals.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Providing credit information services and providing credit references are regulated activities for which firms must be regulated. A firm provides credit information services where it takes (or gives advice in relation to any of the following steps) on behalf of an individual or relevant recipient of credit:

- ascertaining whether a credit information agency holds information relevant to the financial standing of an individual or relevant recipient of credit;
- ascertaining the contents of such information;
- securing the correction of, the omission of anything from, or the making of any other kind of modification of, such information; and
- securing that a credit information agency that holds such information:
    - stops holding the information; or
    - does not provide it to any other person.

Providing credit references involves providing people with information relevant to the financial standing of individuals or relevant recipients of credit where the person has collected the information for that purpose.

In addition, the Small and Medium-Sized Business (Credit Information) Regulations 2015 (the SMB Regulations) require:

- designated banks to share specified credit information about SMEs with designated credit reference agencies (with the permission of the relevant SME); and
- designated credit reference agencies to provide this information to finance providers at the request of the SME and to the BoE.

While the provision of this information is not a regulated activity under the FSMA, the FCA does monitor and enforce compliance with the SMB Regulations.

HMT has proposed to regulate BNPL credit and, potentially, certain forms of short-term interest-free credit under the RAO. The government's ambition is to lay legislation during 2023. As part of HMT's incoming changes to BNPL, it has proposed ensuring that BNPL providers carry out the relevant affordability checks in relation to users and that there is 'clear, consistent and timely credit reporting' across the credit reference agencies in relation to this and it is understood that the FCA will consult on detailed rules for the sector covering affordability checks, licensing of operators, and fair marketing.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

Prior to Brexit, an EEA firm that has been authorised under one of the EU single market directives was able to may provide cross-border services into the United Kingdom. For these purposes, the relevant single-market directives include the:

- Capital Requirements Directive;
- Solvency II Directive;
- second Markets in Financial Instruments Directive;
- Insurance Distribution Directive;
- Mortgage Credit Directive;
- fourth Undertakings for Collective Investment in Transferable Securities Directive;
- Alternative Investment Fund Managers Directive;
- second Payment Services Directive; and
- Electronic Money Directive.

The right to passport into the United Kingdom from EEA jurisdictions ceased to exist after 31 January 2020.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

No. With the removal of passport rights post-Brexit, any firm wishing to obtain a licence in the United Kingdom will need to establish a presence within the jurisdiction.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

The United Kingdom has a comprehensive set of rules relating to financial promotions. These are set out in Chapter 4 of the Financial Conduct Authority's (FCA) Conduct of Business Sourcebook (COBS).

The definition of a financial promotion is very wide and includes an invitation or inducement to engage in investment activity that is communicated in the course of business. Marketing materials for financial services are likely to fall within this definition.

The basic concept is that financial promotions must be fair, clear and not misleading. FCA guidance suggests that:

- for a product or service that places a client's capital at risk, it makes this clear;
- where product yield figures are quoted, this must give a balanced impression of both the short- and long-term prospects for the investment;
- where the firm promotes an investment or service with a complex charging structure or the firm will receive more than one element of remuneration, it must include the information necessary to ensure that it is fair, clear and not misleading and contains sufficient information taking into account the needs of the recipients; the FCA, Prudential Regulation Authority (PRA) or both (as applicable) are named as the firm's regulator and any matters not regulated by either the FCA, PRA or both are made clear; and
- where if it offers 'packaged products' or 'stakeholder products' not produced by the firm, it gives a fair, clear and not misleading impression of the producer of the product or the manager of the underlying investments.

However, an exemption may be available to keep marketing materials outside the scope of the financial promotion rules. For example, exemptions may be available for communications to high-net-worth individuals, companies, sophisticated individuals and other investment professionals. Even authorised firms are prohibited from the promotion of unregulated collective investment schemes, except in specific circumstances set out in the Financial Services and Markets Act 2000 (Promotion of Collective Investment Schemes) (Exemptions) Order 2001 (SI 2001/1060).

Only authorised persons may make financial promotions and it is a criminal offence for an unauthorised person to communicate a financial promotion. Any agreements entered into with customers as a result of an unlawful financial promotion are unenforceable. HM Treasury and the FCA have both consulted on the process for the approval of financial promotions, including introducing a 'regulatory gateway' whereby all new and existing authorised firms will be prohibited from approving the financial promotions of unauthorised persons without having applied to the FCA to have this prohibition removed either entirely (allowing them to approve all types of financial promotions), or partially (allowing them to approve certain types of financial promotions).

The FCA has also recently rationalised the classification of high-risk investments (under the terms restricted mass market investments and non-mass market investments), introducing a package of measures to slow consumer journeys into high-risk investments. The measures introduced include requirements on:

- strengthening risk warnings;
- banning inducements to invest;
- introducing positive frictions;
- improving client categorisation; and
- stronger appropriateness tests.

Lending

In relation to lending, there is also a comprehensive set of rules and the position is similar, but not identical, to that set out in COBS.

In respect of credit agreements, the FCA's Consumer Credit Sourcebook 3.3 applies and provides that a financial promotion must be clear, fair and not misleading. In addition, firms must ensure that financial promotions:

- are clearly identifiable as such;
- are accurate;
- are balanced (without emphasising potential benefits without giving a fair and prominent indication of any relevant risks);
- are sufficient for, and presented in a way that is likely to be understood by, the average member of the group to which they are directed, or by which they are likely to be received;
- are presented in a way that does not disguise, omit, diminish or obscure important information, statements or warnings;
- present any comparisons or contrasts in a fair, balanced and meaningful way;
- use plain and intelligible language;
- are easily legible and audible (if given orally);
- specify the name of the person making the communication (or whom they are communicating on behalf of, if applicable); and
- do not state or imply that credit is available regardless of the customer's financial circumstances or status.

Various other detailed requirements apply depending on the type of credit (eg, peer-to-peer, secured, unsecured or high-cost short-term credit) and the type of agreement (eg, whether it is secured on land), which govern things such as:

- the requirement to include particular risk warnings and how those warnings must be worded; and
- when and how annual percentage rates and representative examples must be included and displayed; and expressions that cannot be included in financial promotions.

In relation to mortgages, chapter 3A of the Mortgages and Home Finance: COBS applies. In addition to being clear, fair and not misleading, financial promotions must:

- be accurate;

Read this article on Lexology

- be balanced (without emphasising any potential benefits without also giving a fair and prominent indication of any relevant risks);
- be sufficient for, and presented in a way that is likely to be understood by, the average member of the group to whom it is directed, or by whom it is likely to be received;
- make it clear, where applicable, that the credit is secured on the customer's home;
- be presented in a way that does not disguise, omit, diminish or obscure important items, statements or warnings; and
- where they contain a comparison or contrast, be designed in such a way that the comparison or contrast is presented in a fair and balanced way and ensures that it is meaningful.

As with credit agreements, other provisions apply depending on the particular type of mortgage, covering, among other things:

- the inclusion and presentation of annual percentage rates and other credit-related information;
- points of contact; and
- when and how financial promotions can be made.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

Regulators in the United Kingdom generally seek to adopt a technology-neutral stance, regulating the outputs of technology systems and the functions or services those systems provide (rather than how they operate). There are no specific rules or regulations concerning the use of distributed ledger technology or blockchain per se.

However, some rules and regulations applicable in the United Kingdom indirectly prevent distributed ledger technology and blockchain from being used in the provision of a particular function or service. For example, the UK General Data Protection Regulation (UK GDPR) generally requires personally identifiable information to be capable of erasure when it is no longer needed, which causes difficulties for firms seeking to use distributed ledger technology to govern the use of that type of data, given the technology's generally 'immutable' (namely, unchangeable) nature. Another example is the UK Central Securities Depository Regulation, which requires transferable securities admitted to regulated trading venues to be represented in book-entry form. This creates a regulatory hurdle for firms seeking to issue or trade transferable securities in digital form (namely, security tokens) on such venues.

Some of the rules and regulations that indirectly prevent the use of distributed ledger technology and blockchains in a financial markets' context will be revisited as part of the UK's forthcoming Financial Markets Infrastructure Sandbox (FMI Sandbox). The FMI Sandbox will allow participating firms to test distributed ledger technology and blockchains in a manner they would not otherwise be permitted, through the granting of temporary exemptions to certain UK rules and regulations (subject to authorisation and ongoing supervision).

Read this article on Lexology

Legislative powers to establish the FMI Sandbox will be granted to UK regulators through the revisions being made to the Financial Services and Markets Act 2000. A consultation paper containing proposals on the scope of the FMI Sandbox is expected over the summer of 2023. The FMI Sandbox is expected to commence later in 2023.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

In the United Kingdom, there are specific rules relating to the operation of certain types of crypto-businesses in the United Kingdom, requiring the following businesses to be registered with the Financial Conduct Authority (FCA):

- those that provide a facility to enable the exchange of one cryptoasset for another or the exchange of fiat currency for cryptoassets (or vice versa), or any business that makes arrangements with a view to any such exchange;
- those that provide custodial cryptoasset wallet services;
- any business that issues new cryptoassets (eg, a business conducting an initial coin offering); and
- businesses that operate cryptoasset automated teller machines.

Prior to operating any such business, the business must first register with the FCA. The registration process is complex and requires the submission of a number of different information requirements. Once a complete application has been submitted, the FCA has three months to consider the application and accept or reject it as it sees fit.

There have proven to be significant challenges in the registration of cryptoasset firms to date. Other regulatory processes regarding cryptoassets continue in other areas.

The FCA's guidelines include a taxonomy covering 'exchange tokens' (decentralised assets such as bitcoin), 'security tokens' (blockchain-traded products that have similar characteristics to traditional regulated securities), and 'utility tokens' (blockchain-traded products or other items that do not have similar characteristics to traditional regulated securities).

Therefore, in broad terms, the current approach in the United Kingdom to the regulation of cryptoassets at present varies with:

- unregulated tokens (classic exchange tokens such as bitcoin and utility tokens) are unregulated, although to offer services concerning them, a business may need to be registered with the FCA;
- e-money tokens (cryptoassets that have the characteristics of e-money) are regulated as if they were e-money, and businesses dealing in them need to be properly authorised by the FCA as appropriate under the Electronic Money Regulations and the Payment Services Regulations, as well as likely needing to be registered with the FCA (depending on what activity is being undertaken in relation to those e-money tokens); and
- security tokens (cryptoassets that have the characteristics of regulated financial products) being regulated in the same way as the type of security that the cryptoasset shares

Read this article on Lexology

characteristics with, and any businesses dealing in them need to be properly authorised by the FCA as appropriate, including being registered with the FCA alongside any wider securities permissions.

E-money institutions that do not issue e-money tokens, but which provide payment services in connection with a cryptoasset (whether or not the cryptoasset is regulated), may need to be authorised under the Payment Services Regulations for these payment services.

Proposed regulatory regime

In February 2023, HM Treasury (HMT) published a consultation on the Future Financial Services Regulatory Regime for Cryptoassets. While this is a consultation and seeks feedback regarding how cryptoassets will be regulated, the consultation shows the direction of travel that HMT intends to take.

The key to the regulatory consultation is a proposal is to bring cryptoassets within scope of existing legislation, rather than create bespoke regulation specific to cryptoassets and activities in relation to them. The consultation proposes to expand the list of 'specified investments' in Part III of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 to include cryptoassets.

HMT confirms that it does not intend to expand the definition of 'financial instrument' in Part 1 of Schedule 2 to the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO) to include presently unregulated cryptoassets. Therefore, while mainly the proposals will mean that existing regulated activities will now apply in relation to cryptoassets in addition to previously specified investments, there are also proposals for some new RAO activities, specific to cryptoassets.

Stablecoins

In relation to stablecoins, HMT is consulting on bringing certain stablecoins within the scope of the UK regulatory perimeter. Specifically, it seeks to regulate 'payment crypto-assets'.

This is intended to cover all fiat currency-backed stablecoins, but exclude those that stabilise their value by referencing other assets (eg, commodities). This will lead to new regulated activities, including the issuing of stablecoins, providing custody for stablecoins, and providing payment services in relation to stablecoins. The FCA will be the regulator for these activities, and firms will need to be authorised. HMT has also proposed an amended financial market infrastructure special administration regime to address the risks posed by the possible failure of systemic digital settlement assets (which would include stablecoin) firms. Further details are awaited.

Financial promotions

HMT has announced that the promotion of cryptoassets to UK consumers is to be regulated and will broadly fall within the FCA's existing financial promotions regime under the Financial Services and Markets Act 2000 (FSMA). The change will come into force on 8 October 2023. The amendments include a broad definition of cryptoassets that capture a significant range of currently unregulated tokens – it would not capture NFTs. It will cover

financial promotions from overseas firms marketing in the United Kingdom, as well as firms that are based in the United Kingdom (even if not authorised by the FCA). For communications originating outside the United Kingdom, the restriction applies to the extent that the communication is capable of having an effect in the United Kingdom.

Promotions to governments and central banks and investment professionals (a specifically defined class of investor) would, however, be exempt. Common retail exemptions on the other hand would not apply, including promotions to high-net-worth individuals or self-certified sophisticated investors.

Together the new rules will mean significant restrictions on the promotion of cryptoassets – financial promotions in relation to these assets will, among other requirements, need to be fair, clear, and not misleading, and include a prescribed risk warning. Only firms registered under the Money Laundering Regulations, or authorised firms will be able to carry out their own promotions in relation to cryptoassets, and only authorised firms will be able to approve unregistered or unauthorised firms' promotions.

Cryptoasset regulation in the United Kingdom continues to be a developing area and the final requirements of the HMT and FCA proposals may change following further consultation.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Any firm that issues a digital token in the United Kingdom needs to be registered with the FCA. The registration process is complex and requires the submission of a number of different information requirements. Once a complete application has been submitted, the FCA has three months to consider the application and accept or reject it as it sees fit.

Beyond the registration requirement noted earlier, there are no rules or regulations specifically governing the issuance of digital tokens. If the token meets the definition of regulated cryptoassets or any other regulated product (even if in tokenised form), Financial Services and Markets Authority and FCA regulations will apply around authorisation and compliance to the same extent that they would apply to traditional assets.

Regulation around cryptoassets in the United Kingdom is undergoing some change at the time of writing including bringing cryptoassets within scope of the UK's regulatory and financial promotion regime. This will include promotions in relation to the issuance of tokens.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

There are not yet any significant rules or regulations that specifically govern the use of artificial intelligence (AI) in the United Kingdom, including in respect of robo-advice. Instead, the rules and regulations that apply to a firm's use of AI depend on the specific nature of the activities for which it is used and, more broadly, any regimes to which a firm is subject at an organisational level.

Fintech firms should consider the status of the activities they are carrying on involving AI under the general licensing regime in the Financial Services and Markets Act 2000 (FSMA). The general prohibition in section 19 of the FSMA prohibits carrying on a regulated activity by way of business in the United Kingdom without authorisation or unless an exemption or exclusion applies. Firms carrying on regulated activities will generally require authorisation by one of the UK's financial services regulators, the most significant of which for fintech firms being the Financial Conduct Authority (FCA), the PRA and the Bank of England (BoE) authorised firms using AI to carry on regulated activities and (or) that use AI in other parts of their businesses will need to consider the relevant regulatory regimes to which they are subject. Under these regulatory regimes, the general rules, guidance, and principles will be relevant to such firms' use of AI as well as specific requirements relevant to particular applications or elements of AI.

At the most general level, firms must have regard to high-level requirements such as the FCA's Principles for Businesses or the Prudential Regulation Authority's (PRA) Fundamental Rules when using AI. For example, the FCA requires firms to communicate with clients in a way that is clear, fair and not misleading and to have adequate risk management systems. Requirements under issue-specific regimes may also apply, for example, governance-related requirements under the Senior Managers and Certification Regime (SMCR) or consumer-protection-related rules for retail clients under the new consumer duty. The SMCR and the consumer duty have been specifically identified by the relevant regulators as the key tools they will use for regulating the use of AI by authorised firms. However, firms should also have regard to other issue-specific regimes especially relevant to AI such as those covering operational resilience, outsourcing, model risk management, and data management. In addition, particular activities may be subject to specific requirements, for example, investment advice provided by robo-advisers, would be subject to conduct of business requirements (eg, suitability assessments and best execution), and systems involved in high-frequency trading decisions would be subject to detailed rules on algorithmic trading.

Although these are existing requirements, their application to the use of AI by businesses requires careful consideration in light of the unique characteristics of AI. The purpose of the BoE-PRA-FCA Discussion Paper 5/22 on AI and machine learning published at the end of 2022 (the Discussion Paper) was to seek views on how existing regulation and legislation may be applied to AI to inform potential future policy proposals. The results of the Discussion Paper are expected at the end of this year but, in the meantime, there are some sources of informal guidance on how existing requirements should apply to AI. The Final

Report of the PRA and FCA AI Public-Private Forum provides examples of best practices on how firms can seek to comply with existing rules on governance, data, and model risk management when using AI. There are also notably two papers published by the FCA on AI in 2019 – 'Explaining why the computer says no' and 'Artificial Intelligence in the board-room'– that emphasise that financial institutions (including their board members) should be able to explain AI-based decisions, particularly in sensitive contexts (eg, in consumer loan applications).

Beyond the financial services regulatory framework, firms using AI will need to consider a number of cross-sectoral rules and regulations that may apply to their activities. The most significant set of cross-sectoral rules and requirements are set out in the UK's data protection regime. Where activities involve processing of personal data, the Data Protection Act 2018 along with the UK GDPR apply minimum standards for data privacy and security. Particularly relevant to firms using AI and robo-advice, the UK GDPR sets out requirements on 'automated' decision-making involving personal data. Article 22 of the UK GDPR provides that a data subject has the right not to be subject to a decision based solely on automated processing except in certain circumstances (eg, with the data subject's explicit consent). Where those circumstances apply, the data controller must provide 'meaningful information about the logic involved'. Firms using personal data in AI (eg, in assessing loan applications) must, therefore, able to explain how the AI system operates in that context. The Information Commissioner's Office (ICO), the UK's data protection regulator, has released extensive guidance on compliance with data protection law when using AI (including the explainability provisions noted above, eg, in its Guidance on AI and Data Protection and AI and Data Protection Risk Toolkit). The ICO has also issued guidance specifically on explaining decisions made with AI in conjunction with the Alan Turing Institute.

Other key cross-sectoral rules and regulations that may apply to firms using AI include those set out in the Equality Act 2010 (the Equality Act) and the Competition Act 1998 (the Competition Act). Discriminatory decisions made involving AI systems could be a breach of the Equality Act. For example, certain AI-derived price-discrimination strategies could breach the requirements if they result in poor outcomes for groups with protected characteristics under the Equality Act. The Equality and Human Rights Commission is the body with primary responsibility for upholding equality and human rights laws in the United Kingdom. Supervisory authorities, though, including the PRA and the FCA, are subject to a public sector equality duty under the Equality Act, which requires them to have regard to the need to eliminate discrimination and other conduct prohibited under the Equality Act, so breaches may also be subject to action from these bodies. The use of AI could also involve breaches of the Competition Act where it results in, for example, anti-competitive behaviour, discriminatory or unfair practices, or cases of abuse of dominance. The Competition and Markets Authority (CMA) is responsible for enforcing the Competition Act but, as with the Equality Act, supervisory authorities, such as the PRA and the FCA, have certain functions under the Competition Act and may use these functions in relation to applications of AI in financial services. In 2019, the CMA published its views on how algorithms, including in the context of AI, can reduce competition and harm consumers and, in May 2023, in line with the UK government's White Paper, it launched a review of competition and consumer protection considerations in the development and use of AI foundation models.

In addition to the aforementioned regulatory considerations, businesses using AI should also be aware of the National Security and Investment Act 2021 (the NSI Act), which came

into force on 4 January 2022. The NSI Act gives the government powers to scrutinise and intervene in business transactions in sensitive areas, including AI, to protect national security. Transactions, including acquisitions, minority investments, and intra-group transactions, involving businesses active in AI may trigger a mandatory requirement to notify the government. In the context of a transaction, such businesses (and any investors) may need to consider whether the transaction triggers a mandatory notification requirement as well as ensuring that any potential implications are reflected in deal timelines and documents to manage the risks of delay and (or) government intervention.

AI, its use by businesses, and its potential impact on societies is an issue attracting increased regulatory and government attention. Unsurprisingly, then, the law and regulation governing the use of AI in the United Kingdom is set to change. In March 2023, the UK government published its White Paper setting out and launching a consultation on its proposals for a regulatory framework for AI. Unlike the approach taken in the European Union, the UK government proposes a flexible and iterative approach beginning with five non-statutory cross-sectoral principles to be interpreted and applied by existing UK regulators through the issuance of guidance on the application of existing laws and regulations to the use of AI. However, in light of the rapid developments and availability of generative AI tools, the UK government is reportedly already considering tightening the position set out in the White Paper to directly regulate the use of AI and create a standalone AI regulator.

In the European Union, the draft AI regulation (AI Act), once implemented, will impose obligations on developers and users of AI systems, particularly those systems classified as 'high risk' under the AI Act. While the AI Act does not specifically target AI use in the financial services sector, fintech businesses could still find themselves subject to potentially onerous obligations under the AI Act, for example, if they use AI in the context of human resources or employment.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Part 12 of the Financial Services and Markets Act 2000 sets out a strict system concerning changes of control of regulated firms, and failure to adhere to the appropriate statutory requirements can be a criminal offence, depending on the nature of the breach.

Controllers or potential controllers of Financial Conduct Authority (FCA)-authorised firms are required to make notifications to and obtain approval from the FCA when a change of control occurs. The notification must be made before a change of control takes place. A person who fails to obtain the appropriate FCA approval will be guilty of a criminal offence.

The notification process takes place under three parallel processes:

- each new controller submitting the appropriate controller notification form to seek the FCA's pre-approval;

- each exiting controller notifying the FCA of the change of control; and
- the FCA-regulated firm notifying the FCA of these changes.

In practice, a joint notification is usually made, coordinated by the FCA-regulated firm with the new controllers and exiting controllers. Any potential controllers must provide detailed information, including in respect of its:

- group structure;
- senior management;
- commercial activities;
- any criminal or civil proceedings against the company; and
- details of the acquisition.

The FCA has a statutory assessment period of 60 working days to determine change-of-control applications. This can be interrupted for a period of 30 days. In practice, determinations are often delayed due to a lack of case officers. The FCA provides an estimate of the current delay on its webpage: at the time of writing this is at least 90 days. The FCA still recommends that all relevant information and documents are provided with the initial submission and reminds firms that it is a criminal offence to proceed with a transaction before it has decided on the notification (or before the statutory assessment period has expired). There is no application fee.

HM Treasury has stated that it, the PRA and the FCA are considering revising change of control applications and it has been suggested that such changes could be focused on:

- the information provided by applicants to enable regulators to fully assess the risks of the proposal in a timely manner; or
- the currently limited statutory grounds on which the FCA or the PRA can object to an application for a change of control.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Generally, fintech companies are only required to have anti-money laundering (AML) procedures if the company is authorised by the Financial Conduct Authority (FCA) or carries out business that is subject to the Money Laundering Regulations 2017 (MLRs). The United Kingdom implemented the EU Fifth Money Laundering Directive (5MLD) on 10 January 2020, by way of updates to the MLRs effected by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (the 2019 Regulations). Under 5MLD, and the 2019 Regulations (in line with 5MLD), the types of entities required to have money laundering procedures have been widened to include cryptoasset exchange providers and custodian wallet providers. The 2019 Regulations also capture peer-to-peer exchange providers, cryptoasset automated teller machines and the issuing of new cryptoassets (eg, an initial coin offering or initial exchange offering).

Read this article on Lexology

Entities subject to UK money laundering regulations are required to, among other things:

- identify and assess the firm's exposure to money laundering risk by, for example, undertaking a risk assessment;
- perform customer due diligence to an adequate standard depending on the risk profile of the customer;
- keep appropriate records;
- monitor compliance with the AML regulations, including internal communication of policies and procedures; and
- report suspicious transactions.

The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022 came into force in 2022 and introduce a number of changes to the 2017 MLRs. Changes that will be particularly relevant to fintech companies are:

- excluding account information service providers from the scope of the 2017 MLRs;
- adding proliferation financing to the list of financial crime risk covered by the 2017 MLRs, meaning that firms subject to the 2017 MLRs will be required to take steps to mitigate the risk of proliferation financing;
- introducing a change in control regime for cryptoasset exchange and custodian wallet providers registered with the FCA under the 2017 MLRs, meaning that prospective acquirers of FCA-registered crypto firms will need to obtain the FCA's approval to the transaction; and
- extending the 'travel rule' for cryptoasset transfers.

As part of its review of fintech challenger banks, the FCA has noted some concerns over the financial crime controls of these companies prompted by the view that criminals may be attracted to the fast onboarding processes that challenger banks advertise and that the risk the information gathered through these fast processes is insufficient to identify higher-risk customers. The FCA noted that it expects financial crime control resources, processes and technology to be commensurate with a bank's expansion so that they remain fit for purpose.

With respect to anti-bribery policies and procedures, all companies (including fintech companies) that are incorporated in or carry on business, or a part of their business, in the United Kingdom, are subject to the Bribery Act 2010 (the Bribery Act). While the Bribery Act does not require the implementation of policies or procedures to combat bribery, it creates a de facto requirement to do so. This is because a company charged with 'failing to prevent bribery' may rely on the statutory defence that the company had adequate policies and procedures in place designed to prevent bribery. It is not just large companies that need to be concerned with this law. The successful prosecution of Skansen Interiors Ltd (a company with fewer than 30 employees) for failing to prevent bribery in 2018 indicates that UK prosecutors will target smaller companies for such an offence.

From 1 September 2023, the 'travel rule', which requires financial institutions to share identifying information about the originator and beneficiary of a transaction, will apply to transfers of cryptoassets in the United Kingdom, bringing the United Kingdom in line with Financial Action Task Force Recommendation 16 regarding information sharing requirements for transferring cryptoassets. Cryptoasset exchange providers and custodian wallet providers registered with the FCA will be subject to the rule when they provide services to

Read this article on Lexology

the originator or beneficiary of a transfer of cryptoassets. Different cryptoasset transfers will attract different requirements as to the information that the originator's cryptoasset service provider must be shared alongside the transfer. Cross-border cryptoasset transfers with a value exceeding €1,000 will require additional information and transactions with self-hosted wallets may also attract additional requirements depending upon the firm's assessment of the risk.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

There is no anti-financial crime guidance issued by the FCA specifically for fintech firms. However, firms that are authorised by the FCA should comply with its 'Financial Crime Guide: A firm's guide to countering financial crime risks', and may find the FCA's feedback on good and poor quality applications for registration under the 2017 MLRs helpful. In addition, the Joint Money Laundering Steering Group (JMLSG) issues detailed AML guidance for the financial sector, which includes a chapter of guidance specific to the cryptoasset sector (see Chapter 22 of Part 2 of the JMLSG Guidance).

It is important for fintech firms to understand the concerns and policy drivers that financial institutions have with respect to their fintech clients. In June 2018, the FCA sent a 'Dear CEO' letter to financial institutions, advising them to take 'reasonable and proportionate measures to lessen the risk of your firm facilitating financial crimes that are enabled by cryptoassets'. This will have a consequential effect on fintech companies, as financial institutions are likely to apply the FCA's guidance when conducting due diligence on and monitoring their relationships with crypto-businesses as a result of this letter. While not addressed to fintech companies, they may also find this guidance helpful in mitigating financial crime risks in their own relationships with individuals and entities whose wealth, funds or revenue derives from crypto-related activities. More recently, the FCA sent a 'Dear CEO' letter to firms regulated under the Payment Services Regulation 2017 and Electronic Money Regulations 2011, identifying three 'outcomes' that the FCA wants those firms to achieve, with financial system integrity through anti-money laundering and sanctions measures being one such outcome. The FCA's letter identifies common financial crime issues that the FCA has observed at firms and the action that it expects firms to take to address those issues.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

On 25 May 2018, the GDPR came into force with direct effect across the entire European Union. In the United Kingdom, the Data Protection Act 2018 came into force at the same time as the GDPR and supplemented the GDPR as it applied in the United Kingdom. Following Brexit, the GDPR took effect in the United Kingdom as the 'UK GDPR', which is the retained EU law version of the GDPR as amended by various data protection EU exit

regulations. The Data Protection Act 2018 now supplements the UK GDPR. The government has published Keeling Schedules showing the changes (in redline form) to the EU GDPR and the Data Protection Act 2018 made by the data protection EU exit regulations. These schedules are not law but are a useful guide to how the UK GDPR and the Data Protection Act 2018 now look.

Going forward, for any entity in the United Kingdom, one or both of the UK GDPR or the EU GDPR (together, the GDPR) may apply, depending on what activities that entity carries out, and it will need to be established whether any entity is subject to one or both regimes. Currently, the UK GDPR and the EU GDPR obligations continue to be very similar or the same, but this should be kept under constant review.

The GDPR governs the storage, viewing, use of, manipulation and other processing by businesses of data that relates to a living individual. In summary, the GDPR requires that businesses may only process personal data where that processing is done in a lawful, fair and transparent manner, as further described in the GDPR.

The GDPR requires that any processing of personal data must be done pursuant to one of the available lawful bases for processing. One of the most commonly used lawful bases for processing is to obtain the consent of the data subject to that processing – in relying on this lawful basis, the business must ensure that the consent is freely given, specific, informed and unambiguous, and capable of being withdrawn as easily as it is given. This places a significant burden on businesses to ensure that their customers are fully informed as to what their personal data is being used for. Other lawful bases for processing data include where that processing is necessary for the business to perform a contract it has with the data subject, where the business has a 'legitimate interest' in processing the personal data (which is not overridden by the 'fundamental rights and freedoms' of the data subject) or where required to comply with an obligation the business has at law (not a contractual obligation).

The GDPR does not apply to personal data that has been truly anonymised – as anonymised data cannot, by definition, be personal data. However, to ensure that GDPR does not apply to a certain data set, that data set must be truly anonymised. The GDPR itself gives limited guidance on anonymisation in Recital 26, requiring data controllers to consider a number of factors in deciding if personal data has been truly anonymised, including the costs and time required to de-anonymise, the technology available at the time to attempt de-anonymisation and further developments in technology.

Businesses that infringe the GDPR may be subject to administrative fines of an amount up to €20 million under the EU GDPR (£17.5 million under the UK GDPR) or 4 per cent of global turnover, whichever is higher. If an entity is subject to both the UK GDPR and the EU GDPR, it is possible for the entity to be fined under both regimes for the same breach.

The oversight of UK businesses' compliance with the UK GDPR and related legislation, and enforcement of them, is carried out by the UK regulator, the Information Commissioner's Office. If a UK business has operations in the European Union that mean it is subject to the EU GDPR, it may need to appoint a representative in the EU member state in which those operations are most significant, and the oversight of UK businesses' compliance with the EU

Read this article on Lexology

GDPR and related legislation, and enforcement of them, generally will be led by the relevant regulator in that EU member state.

There are restrictions under both the EU GDPR and the UK GDPR on transfers of personal data to non-EU or UK countries that are not deemed to offer a standard of protection by the European Commission or the UK government (as applicable). Unless a derogation under article 49 of the GDPR is available, a suitable data transfer mechanism will be needed to legitimise such transfers. The most common method of legitimising these transfers is the entry into 'standard contractual clauses', as approved by the European Commission or UK government (as applicable). Following the *Schrems II* judgment, businesses are now also required to carry out a 'transfer impact assessment', which requires businesses to review whether any supplementary measures are needed to ensure that transfers relying on the standard contractual clauses (or 'binding corporate rules') provide adequate data protection for the personal data in practice.

In June 2022, the government published its long-awaited plans to reform the UK Data Protection Act 2018, following the Queen's Speech in May 2022, in which it announced that it saw the bill as an opportunity to create a more 'pro-growth and pro-innovation data regime while maintaining the UK's world-leading data protection standards'. Since then there have been a number of announcements seeking to reform the existing UK data protection regime following Brexit, including the Data Protection and Digital Information (No. 2) Bill, which was introduced into Parliament in March 2023. While the Bill is at the time of writing undergoing Parliamentary scrutiny, the overarching pro-innovation and growth principles of the Bill have been well received.

There are no rules or regulations in the United Kingdom relating to personal data that are specifically aimed at fintech companies.

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

There are no rules or regulations in the United Kingdom that provide cybersecurity requirements for fintech businesses specifically. More generally, the UK GDPR imposes requirements on businesses in the United Kingdom to ensure a high standard of security over personal data that they process, including the general obligation to have in place reasonable technical and organisational measures to ensure the security of that data, compliance with which requires measures relating to cybersecurity to be put in place.

Further, for FCA-regulated businesses, the FCA has significant powers of oversight and enforcement in respect of those businesses' internal systems and controls relating to the protection of confidential client information. The FCA actively manages and oversees these requirements and, in recent years, has imposed significant fines on entities that have failed to meet these requirements.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

The position on regulation of outsourcing by financial services companies in the United Kingdom is a complex picture, encompassing a number of different requirements that apply in different ways, depending on the type of financial services business in question.

The most important of these requirements are the European Banking Authority (EBA) guidelines. On 25 February 2019, the EBA published revised (final) guidelines on outsourcing arrangements (the Guidelines) for credit institutions and certain investment firms as well as payment and e-money institutions. The Guidelines amend and finalise previously published draft guidelines in light of extensive consultation responses from the industry and industry bodies. Therefore, the Guidelines are consistent with, and build upon, the previous Senior Management Arrangements, Systems and Controls Chapter 8 (SYSC 8) requirements within the Financial Conduct Authority (FCA) Handbook (which now operate mostly as guidance rather than as requirements); however, they apply to a broader set of businesses than SYSC 8 – most noteworthy is the inclusion of payment and e-money institutions, which are not subject to SYSC 8.

In broad terms, the Guidelines provide more granular detail around requirements that relevant businesses must comply with when carrying out outsourcing (including in relation to internal processes and procedures), compared to the SYSC 8 requirements.

The Guidelines took effect on 30 September 2019 and have been adopted in the United Kingdom. All new outsourcing contracts entered into after this date should be compliant with the Guidelines, and relevant institutions are expected to review and update any internal processes and procedures to meet the Guidelines' requirements. Companies that did not finalise remediations of existing contracts by 31 March 2022 are obliged to inform the FCA, as the FCA confirmed that the original hard deadline set by the EBA of 31 December 2021 no longer applied in the United Kingdom. The Guidelines support the harmonisation of existing regulation and guidance applicable to different types of financial services firms.

The Prudential Regulation Authority (PRA) and the FCA have also published supervisory statements (Statements) that build on the Guidelines and set out the PRA and the FCA's expectations as to how UK firms will implement outsourcing regulation and manage outsourcing risks, as well as certain other material or high-risk third-party arrangements that are outside the scope of the Guidelines. The Statements make up part of the PRA and the FCA's wider focus on operational resilience and aim to ensure firms have robust structures and processes in place to manage third-party risk.

Firms that are regulated by the PRA were expected to comply with the expectations in the PRA Statements by 31 March 2022, mirroring the deadline set by the FCA. These expectations are broadly in line with the Guidelines but expand the scope to certain third-party arrangements.

Read this article on Lexology

In April 2021, the Bank of England (BoE) published three consultation papers on the requirements that must be met for outsourcing and third-party arrangements for Financial Marker Infrastructure (FMI) entities, which appears to extend the expectations under the PRA Statement to FMI entities. The BoE issued a policy statement in February 2023 providing feedback in response to the three consultation papers, publishing final Supervisory Statements for outsourcing and third-party risk management for different forms of FMI's, and a Code of Practice for Recognised Payment Operators and Specific Service Providers. The FMI's will be expected to comply with expectations in their respective Supervisory Statement or Code of Practice by 9 February 2024, and any outsourcing agreements entered into on or after 8 February 2023 will be expected to meet the Supervisory Statement before then.

Operational resilience

Operational resilience is a third pillar of financial regulation concerning banks and other financial services firms, defined by the PRA as 'the ability of firms, FMI's and the sector as a whole to prevent, respond to, recover and learn from operational disruptions'.

In the United Kingdom, last year, the UK financial regulators issued new policy and supervisory statements on operational resilience, which came into force in March of this year impacting investment firms, banks, insurers, and branches of non-UK firms operating in the United Kingdom, including the PRA's supervisory statement SS1/21 'Operational Resilience: Impact tolerances for important business services', which requires firms to prepare for 'severe but plausible risks' in connection with important business services. Since then, further consultation papers have been issued indicating the extension of the scope of regulation to a broader range of market participants (such as payment service providers and financial market infrastructure providers) and there is currently discussion in the United Kingdom on the extension of regulatory oversight to critical third-party technology suppliers. The approach the UK regulators have taken is to focus on the resilience of the important products or services offered by the firm to the market.

The rules proposed under the consultation papers apply to all third-party service provision arrangements, which is wider than just outsourcings. Among other things, the FCA identified concentration risks (eg, dependency on a particular service provider within the financial services sector) and global service providers with inconsistent resilience requirements across various countries, as key areas of risk from an operational resilience perspective.

Traditionally regulated financial entities will be subject to both the PRA and the FCA operational resilience requirements, whereas a select few firms (including UK investment exchanges) will only be subject to the FCA requirements. On the premise that the occasional operational disruption is unavoidable, both regulators expect firms to govern their operations accordingly by taking the following steps during the three-year transitional period starting on 31 March 2022:

- Firms must identify their important business services and establish impact tolerances for each service, determined by the maximum period of time a service can be disrupted before it impacts the stability of the firm, customer, or the financial sector as a whole. The firm must implement strategies, processes and systems accordingly.

Read this article on Lexology

- Map the resources that are fundamental to supporting important business services and test their capabilities to perform within the relevant impact tolerance throughout a range of plausible disruption scenarios.
- Use the testing data or information garnered from a disruption to perform a 'lessons learned' exercise to identify weaknesses and where to prioritise improvements.
- Firms will then be required to prepare and keep up to date a written self-assessment of their compliance with the operational resilience requirements, and maintain internal and external communications including clear and timely communications to relevant stakeholders in the event of a disruption.
- Ensure the regular engagement of boards and senior management in setting effective standards for the management of operational resilience, and further ensure those firm members have the required expertise and training to discharge their respective resilience responsibilities.

By 31 March 2025, the PRA and the FCA expect firms to approach operational resilience as a dynamic governance activity and have established a clear, comprehensive strategy against operational risk aligned with their respective regulation framework.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

There are no specific legal requirements in the United Kingdom regarding the use of cloud computing in the financial services industry. However, there does exist a body of guidance on the subject and a number of legal requirements that apply to indirectly regulate the use of cloud computing in financial services.

The primary legal requirements relevant to this question relate to the EBA Guidelines and other outsourcing requirements, which apply to financial services businesses when outsourcing material functions. In many different contexts, the use of cloud services will be of sufficiently significant importance to the business's operations to bring this requirement into scope and require the business to meet those outsourcing requirements in undertaking outsourcing. In particular, the European Securities and Markets Authority (ESMA) published guidelines on outsourcing to cloud service providers on 10 May 2021 (the ESMA Guidelines). The ESMA Guidelines are intended to ensure that firms and competent authorities identify, address, and monitor their cloud outsourcing arrangement risks. As with the EBA Guidelines, the ESMA Guidelines provide more granular detail around requirements that relevant businesses must comply with when carrying out outsourcing, with a particular focus on information security requirements in their internal policies, including the protection of confidential, personal, or otherwise sensitive data. The guidelines took effect from 31 July 2021 and apply to all cloud outsourcing arrangements entered into, renewed, or amended on or after this date, and firms should review and amend existing cloud outsourcing arrangements by 31 December 2022.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Computer programs (and preparatory design materials for computer programs) are protected by copyright as literary works. Copyright arises automatically as soon as the computer program is recorded. No registration is required.

Databases underlying software programs may also be protected by copyright and, in certain circumstances, by database right. Database right is a standalone right that protects databases that have involved a substantial investment in obtaining, verifying or presenting their contents (see section 14(1) of the Copyright and Rights in Databases Regulations 1997). Both database copyright and database rights arise automatically without any need for registration.

If the software code has been kept confidential, it may also be protected as confidential information. No registration is required.

Programs for computers, and schemes, rules or methods of doing business 'as such', are expressly excluded from patentability under the Patents Act 1977 (PA 1977). These exclusions ultimately flow from the European Patent Convention. Notwithstanding these exclusions, it is possible to obtain patents for computer programs and business methods if it can be shown that the underlying invention makes a 'technical contribution' over and above that provided by the computer program or business method itself, such as an improvement in the working of the computer. Accordingly, a well-drafted patent may be able to bring a computer-based, software or business method invention within this requirement, but this may be difficult to do and will not always be possible. Registration formalities must be followed to obtain protection.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Copyright and database rights created by an employee in the course of their employment are automatically owned by the employer unless otherwise agreed (see section 11(2) of the Copyright, Designs and Patents Act 1988). Inventions made by an employee in the course of their normal duties (or, in the case of employees who owe a special obligation to further the interests of their employer's business, in the course of any duties) are automatically owned by the employer (section 39 of PA 1977).

However, copyright and inventions created by contractors or consultants in the course of their duties are owned by the contractor or consultant unless otherwise agreed upon in writing.

Database rights are owned by the person who takes the initiative and assumes the risk of investing in obtaining, verifying and presenting the data in question. Depending on the circumstances, this is likely to be the business that has retained the contractor or consultant.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Restrictions on a joint owner's ability to use, license, charge or assign its right in intellectual property will depend on the intellectual property right in question. For example, the restrictions on a joint owner of a patent are different from those on a joint owner of copyright.

A joint copyright owner cannot copy, license or grant security over a jointly owned copyright without the consent of the other joint owners (see sections 16(2) and 173(2) of the Copyright, Designs and Patents Act 1988). Each joint owner may assign their own interest, but consent is required for an assignment of the whole right. A joint copyright owner is also able to grant security over their interest.

In the case of UK patents and patent applications, a joint owner is entitled to work the invention concerned for his or her own benefit and does not need the consent of the other joint owners to do so (section 36(2) of PA 1977). However, the consent of the other joint owners is required to grant a licence under the patent or patent application and to assign or mortgage a share in the patent or patent application (section 36(3) of PA 1977).

The situation is similar for UK-registered trademarks. Each joint owner is entitled to use the registered trademark for their own benefit without the consent of the other joint owners (section 23(3) of the Trade Marks Act 1994 (TMA 1994)), but the consent of the other joint owners is required to grant a licence of the trademark and to assign or charge a share in the trademark (section 23(4) of TMA 1994).

Given the variations in the rights and restrictions of joint owners, and given that the rights of joint owners also differ on a country-by-country basis, it is highly advisable in any situation where parties work together on a project to agree at the outset how the results are to be owned by the parties and their individual rights to exploit the results. In general, joint ownership of intellectual property should be avoided if possible because of the complexities described earlier.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Protection of trade secrets in the United Kingdom is regulated by the Trade Secrets (Enforcement, etc) Regulations 2018 (the Trade Secrets Regulations), which implemented the EU Trade Secrets Directive in the United Kingdom and came into force on 9 June 2018. Trade secrets are also protected by the law on breach of confidence, which provides broadly the same level of protection as is required under the Trade Secrets Directive. The Trade

Secrets Regulations define what qualifies as a protectable trade secret, providing protection for information that:

- is secret, in the sense that it is not generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question;
- has commercial value because it is secret; and
- has been subject to reasonable steps (under the circumstances) by the holder of the information to keep it secret.

The Trade Secrets Regulations also implemented aspects of the EU Trade Secrets Directive that differed from, or added to, the existing law applying to the protection of confidential information. This includes specifying the limitation period for bringing a trade secrets claim and the rules regarding awarding damages and interim and corrective measures.

Confidential information (which may include non-public information that is not captured by the definition of 'trade secret') can be protected against misuse, provided the information in question has the necessary quality of confidence and is subject to an express or implied duty of confidence. In the case of both trade secrets and confidential information, no registration is necessary (or possible). Trade secrets and confidential information can be kept confidential during civil proceedings with the permission of the court.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Brands can be protected as registered trademarks in the United Kingdom. Following Brexit, it, is no longer possible to protect a brand in the United Kingdom via an EU trademark. A brand can also be protected under the common law tort of passing off if it has acquired sufficient goodwill.

Certain branding, such as logos and stylised marks, can also be protected by design rights and may also be protected by copyright as artistic works.

The UK database can all be searched to identify registered or applied for trademark rights with effect in the United Kingdom. It is highly advisable for fintech businesses to conduct trademark searches to check whether earlier registrations exist that are identical or similar to their proposed brand names. It may also be advisable to conduct searches of the internet for any unregistered trademark rights that may prevent the use of the proposed mark.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

Remedies include:

- preliminary and final injunctions;

- damages or an account of profits;
- delivery up or destruction of infringing products;
- publication orders; and
- costs.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

Competition authorities in the United Kingdom (and elsewhere) face a range of potentially complex competition law issues in relation to fintech offerings. These include:

- the risk of anti-competitive collusive behaviour between undertakings through partnerships or industry initiatives (including environmental, social and corporate governance
- initiatives);
- the risks around the exchange of competitively sensitive information;
- the risks of a fintech firm or platform obtaining a dominant position in the market and any behaviour that could potentially exclude or exploit other market players;
- the development and participation in technical standards;
- exclusivity arrangements between parties to a fintech offering;
- the limits of any specified tying or bundling of products or services to the fintech solution; and
- issues around the anticompetitive use of algorithms and machine learning.

The Competition and Markets Authority (CMA), the Financial Conduct Authority (FCA) and the Payment Systems Regulator (all of which are concurrent competition law enforcement authorities in the United Kingdom) generally consider fintech to represent a pro-competitive force, leading to change in markets and encouraging innovation. For example, the FCA is an active participant in the Global Financial Innovation Network.

However, the CMA has been undertaking a number of initiatives to formulate its approach to the regulation of competition in the UK digital markets – including fintech – with a view to focusing on the protection of the consumer.

Since undertaking an investigation into the retail banking market and the implementation of the Open banking remedies (intended to improve the quality of the information provided to customers), the CMA has also taken advice from external experts, advocating a more involved approach to competition regulation. More specifically, the CMA was advised to perform more sophisticated analyses of digital mergers, consider the role of big data in creating barriers to entry, and take account of network effects to create more effective rules for large digital platforms (see the Furman and Lear reports for further information).

As a result, the CMA issued its initial Digital Markets Strategy in June 2019, which recognised the profound changes taking place across the economy, and society more widely, as a result of the growth of digital markets. It set out the CMA's priorities for its digital work

to address these changes and ensure consumers continue to get good outcomes in those markets through competition and innovation. The Digital Markets Strategy was refreshed in February 2021 in light of the market changes that had taken place – not least, the government's decision to establish a Digital Markets Unit (DMU) within the CMA. The DMU was subsequently established within the CMA on 7 April 2021 to focus on operationalising and preparing for the new regulatory regime to be legislated. The intervening period had also seen the CMA – among other things:

- create a Digital Markets Taskforce: a dedicated unit with the role of monitoring developments in digital markets and advising the government on how best to approach them;
- work with Ofcom and the Information Commissioner's Office to established the Digital Regulation Co-operation Forum (DRCF) to support cooperation and coordination on online regulatory matters, and enable coherent, informed and responsive regulation of the UK digital economy (the FCA joined as a full member in April 2021). The DRCF has since published its '2023/24 workplan', which set out the organisation's key areas of focus for 2023–2024. These are to increase promote competition and data protection, increase online safety and support effective governance of algorithmic systems;
- revise its Merger Assessment Guidelines to ensure that the way in which digital technologies have affected how goods and services are delivered to customers, and how businesses compete with each other, is properly reflected in assessing whether a merger could harm consumers. In particular, the new guidelines seek to address the competition challenges arising from two-sided markets, the potential for digital input foreclosure, and potential or dynamic theories of competitive harm; and
- increase its data and behavioural science capabilities through the work of its DaTA unit, including launching an analysing algorithms programme.

On 9 March 2022, the government published its Plan for Digital Regulation, which aimed to drive agile regulation, offering clarity and confidence to consumers and businesses. Regulation was to be underpinned by three principles:

- actively promoting innovation;
- achieving forward-looking and coherent outcomes; and
- exploiting opportunities and addressing challenges in the international arena.

Following this consultation process, in April 2023, the Digital Markets, Competition and Consumers (DMCC) Bill was published in draft form. The DMCC Bill is a piece of UK legislation that aims to promote free and fair competition among businesses, both online and offline, while also protecting consumers from unfair practices. The Bill is likely to come into effect in the second half of 2024. There are three primary areas of focus for the legislation (which applies to the fintech sector just as any other), namely:

- consumer protection: empowers the CMA to take enforcement action against businesses that use unfair practices to deceive consumers, such as fake reviews, subscription traps and pressure selling;
- digital markets: the Bill establishes a new regime overseen by the DMU within the CMA, which is designed to hold digital firms accountable for their actions and prevent firms with 'strategic market status' (considered in the current draft legislation to be 'substantial and entrenched market power and a position of strategic significance in respect of

the digital activity') from using their size and power to limit digital innovation or market access; and
- the DMCC Bill: aims to promote competition in the economy more broadly. It gives the CMA stronger investigative and enforcement powers, which allows it to conduct faster and more flexible competition investigations, and identify and stop unlawful anti-competitive conduct more quickly.

The CMA has also continued in its increasingly interventionist stance in UK merger cases. This more interventionist approach has been present in all sectors to some extent, but it has been particularly noticeable in relation to fintech deals as it is seen to play an important role in the UK's post-Brexit standing as a global financial centre. Over the past few years, a number of in-depth investigations have been related to transactions involving fintech players (eg, FNZ's acquisition of GBST, PayPal's acquisition of iZettle, and the merger of Crowdcube and Seedrs). Innovation and potential (future) competition theories of harm are very much at the forefront of the CMA's merger analyses.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

The United Kingdom has introduced a wide range of tax incentives that are available to fintech companies and investors in such companies. The key incentives are set out below, although there are a number of conditions to be met to qualify for each scheme:

- seed enterprise investment scheme (SEIS): 50 per cent income tax relief and exemption from capital gains tax for investors in high-risk start-up trading companies;
- enterprise investment scheme (EIS): 30 per cent income tax relief and exemption from capital gains tax for investors in small high-risk trading companies;
- venture capital trust (VCT) scheme: 30 per cent income tax relief and exemption from capital gains tax for investors in venture capital trusts, which subscribe for equity in, or lend money to, small unquoted companies;
- business asset disposal relief (formerly entrepreneurs' relief): a reduced 10 per cent capital gains tax rate for entrepreneurs selling business assets (only available to directors and employees of businesses);
- investors' relief: a reduced 10 per cent capital gains tax rate that allows other types of shareholders to benefit from the same relief as is provided under business asset disposal relief when they sell their shares. Unlike business asset disposal relief, this reduced rate is only available to investors who have not been officers or employees in the company whose shares are being sold;
- research and development tax credits: tax relief for expenditure on research and development;
- patent box regime: a reduced 10 per cent corporation tax rate for profits from the development and exploitation of patents and certain other intellectual property rights;
- innovative finance individual savings account (ISA) eligibility: peer-to-peer (P2P) loans are eligible for inclusion in tax-free ISAs;

- tax relief for P2P bad debt: an income tax relief for irrecoverable P2P loans, or P2P bad debt; and
- P2P interest withholding tax exemption: P2P loan interest payments are exempt from UK withholding tax.

A company may raise up to £250,000 (increased from £150,000 from April 2023) under the SEIS and up to a total of £5 million (£10 million for knowledge-intensive companies) over 12 months from 'relevant investments', which includes investments under the SEIS and EIS and investments by VCTs (subject to a lifetime limit of £12 million or £20 million). While financial activities are an excluded activity for the SEIS, EIS and VCT scheme, as long as a fintech company is only providing a platform through which financial activities are carried out, such a fintech company should still qualify for those schemes assuming it meets the other conditions.

For expenditure incurred on or after 1 April 2023, the R&D Expenditure Credit rate increased from 13 per cent to 20 per cent, the small and medium-sized enterprise (SME) additional deduction rate reduced from 130 per cent to 86 per cent, and the SME payable credit rate (for non-R&D intensive companies) decreased from 14.5 per cent to 10 per cent.

The government also published details of a new R&D scheme for qualifying 'R&D intensive' SMEs from 1 April 2023. Eligible R&D-intensive SMEs are able to claim an additional higher R&D payable credit rate of 14.5 per cent instead of the 10 per cent credit rate for non-R&D intensive companies. An 'R&D intensive' company is a 'loss-making SME with an R&D intensity of at least 40%' (meaning that such company incurs at least 40 per cent of its expenditure on R&D). Legislation will be included in the Finance Act 2023.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

The headline rate of UK corporation tax increased from 19 per cent to 25 per cent from April 2023.

The government continues its review of the UK funds regime that could result in wide-ranging changes to the tax and regulatory frameworks for investment funds in the United Kingdom. In addition, Budget 2020 announced a review of how financial services are treated for value added tax (VAT) purposes and the European Commission has also launched a similar review. Fintech companies are advised to keep an eye on what emerges from these reviews, given the potential impact on their tax position.

The digital services tax (DST) was introduced on 1 April 2020 following a government consultation. This 2 per cent tax applies to the revenues of search engines, social media services and online marketplaces, which derive value from UK users. The DST applies where a group's worldwide revenue from digital activities is more than £500 million and more than £25 million of the revenue is derived from the United Kingdom. As such, the tax is expected to impact a small number of large multinationals. Financial services providers are excluded from the online market places definition, meaning fintech companies should generally fall out of the scope of this tax. However, where there are unified platforms with social

media, marketplace and search engine elements and the threshold conditions are met, then fintech companies could fall in scope for revenue from the social media and search engine income streams. It is expected that the UK DST will be replaced in the longer term by the introduction of multinational rules based on Organisation for Economic Co-operation and Development (OECD) Pillar One.

The government recently consulted on merging the two existing R&D expenditure incentive schemes. The government has indicated it will publish draft legislation on a possible merged scheme for technical consultation in summer 2023 with potential implementation from April 2024.

Changes are being made to the UK's transfer pricing documentation requirements, which will align them with the OECD Transfer Pricing Guidelines. This measure will primarily affect businesses operating in the United Kingdom, which are part of a large multinational enterprise group that has global revenues of €750 million or more and will have effect for accounting periods commencing on or after 1 April 2023 for corporation tax purposes.

A multinational top-up tax and domestic top-up tax will be introduced for groups with annual global revenues exceeding €750 million where they are conducting business activities in the United Kingdom. These top-up taxes form the first stage of the UK's implementation of the OECD's Pillar Two rules. The objective of Pillar Two is to implement a global minimum level of taxation for corporate entities at an effective rate of 15 per cent. The multinational top-up tax will target UK parent companies within a multinational enterprise group. The top-up tax will be triggered where:

- a UK parent company has an interest in entities overseas in a non-UK jurisdiction; and
- the UK parent company's group has profits arising in such non-UK jurisdiction that are taxed below 15 per cent.

The domestic top-up tax will target UK companies. The domestic top-up tax will be triggered where the company or group's profits in the United Kingdom are taxed below 15 per cent. In essence, the UK government considers that if UK companies are to be subject to a top-up tax, the UK Exchequer should benefit from it. The measures will have effect for accounting periods beginning on or after 31 December 2023.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

All non-UK nationals, save for Irish nationals, need permission to work in the United Kingdom.

The Skilled Worker visa is most relevant. A candidate needs an offer from a licenced sponsor and the role must meet minimum skill and salary criteria. A lower salary may be paid where the worker is aged under 26, has a relevant PhD or STEM PhD or the role is a specified

shortage occupation. IT business analysts, architects and system designers, programmers and software development professionals, web design and development professionals and cyber security specialists are currently shortage occupations but finance roles are not.

Licenced sponsors with linked overseas entities, may use the Global Business Mobility (GBM) route, including the Senior and Specialist Worker category. The minimum skill and salary levels for the UK role are higher than for a Skilled Worker and the worker must have at least 12 months service with the linked overseas employer unless they are a high earner.

The GBM Secondment Worker route is for those being seconded to the United Kingdom as part of a high-value contract or investment by their overseas employer. However, there are stringent financial thresholds that will limit the use of this route.

The GBM UK Expansion Worker route is the route for those looking to set up a company in the United Kingdom. It can only be used by businesses who are not yet trading in the United Kingdom and requires the worker to be sponsored by a branch or wholly owned subsidiary of an established overseas business. The same minimum skill and salary criteria and overseas employment criteria apply as for the GBM Senior and Specialist Worker route.

Founders of an innovative scalable company in the United Kingdom may be eligible for the new Innovator Founder visa (formerly the Innovator visa but incorporating elements of the now closed Start-Up visa). Business plans must be endorsed by a UK-authorised body but there is no requirement for initial capital to invest in the business and visa holders can undertake additional skilled work.

A Global Talent visa (Digital Technology) is an option where an individual has technical or business skills in the digital technology sector and is endorsed as a leader in their field. Such endorsement is currently by Tech Nation.

The High Potential Individual visa is for recent graduates from institutions named on the UK Visas and Immigration Global Universities List. Crucially, no sponsorship is required, applicants do not need to have a job offer and can work in any capacity. This route is therefore particularly useful for employers who do not yet have a sponsor licence. For other graduates, there is the Graduate visa. Students, sponsored by a UK institution, who have completed a UK degree or other eligible course may apply. The employer does not need to sponsor the individual and they can work in any role for up to two years following which they can switch into a Skilled Worker visa.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

The authorities in the United Kingdom continue to develop their approach to the regulation of fintech businesses.

Over the next 12 months, the UK legislative and regulatory authorities are expected to focus considerable attention on the regulation of cryptoassets, enforcing the consumer duty, gaining a better understanding of banking as a service or embedded finance models and increasing protection from authorised push payment fraud.

In February 2023, The Financial Conduct Authority (FCA) and the Bank of England (BoE) BoE published their latest regulatory grid to help financial firms prepare for upcoming regulatory work planned by the UK's legislative and regulatory bodies, including the government, the FCA, the BoE, the Competition and Markets Authority and the Payment Services Regulator. Upcoming regulatory developments relevant to the fintech sector include:

- the coming into force is the new consumer duty, which will apply to all regulated firms who either face retail clients or customers directly or manufacture products for such customers (including digital banks, robo-advisers and insurers as well as payments, e-money and crypto firms) at the end of July 2023;
- consultations on rules for the stablecoin regime, the future regulatory regime for cryptoassets, and oversight of critical third parties;
- further consultation by the BoE on the potential introduction of a UK central bank digital currency;
- the expansion of a new financial markets infrastructure sandbox to support firms wishing to use new technology such as distributed ledger technology to provide infrastructure services to the financial markets;
- a consultation and draft legislation on the regulation of buy-now, pay-later. The new legislation is expected to be introduced in 2023;
- a response to the consultation on the opportunities and risks arising from open finance and the FCA's role in ensuring that it develops in the best interests of consumers;
- publication of further measures to help prevent authorised push payment scams and the reimbursement regime for such scams, focusing on the implementation of systems to provide confirmation of payee services starting for some firms from the third quarter of 2023;
- a call for evidence on the Payment Services Regulations Review;
- publication of a consultation paper on incident and outsourcing reporting arrangements; and
- a consultation on new access to cash legislation expected in the summer of 2023.

* *The authors wish to thank Minesh Tanna, Angus Brown, Ben Foster, Viktorija Kasper, Gary Barnett, David Trapp and Jo Crookshank for their assistance in the preparation of this chapter.*

George Morris	george.morris@simmons-simmons.com
Oli Ward	oliver.ward@simmons-simmons.com
Sophie Sheldon	sophie.sheldon@simmons-simmons.com
Olly Jones	olly.jones@simmons-simmons.com
Gordon Ritchie	gordon.ritchie@simmons-simmons.com

Citypoint, 1 Ropemaker Street, London EC2Y 9SS, United Kingdom
Tel: +44 20 7628 2020
www.simmons-simmons.com

Read more from this firm on Lexology

Read this article on Lexology

United States

Casey J Jennings, Paul T Clark, Jeffrey M Berman, Beth H Alter and Seth Kuntz*

Seward & Kissel LLP

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES 707

General innovation climate 707
Government and regulatory support 708

FINANCIAL REGULATION 709

Regulatory bodies 709
Regulated activities 710
Consumer lending 710
Secondary market loan trading 711
Collective investment schemes 711
Alternative investment funds 711
Peer-to-peer and marketplace lending 712
Crowdfunding 712
Invoice trading 713
Payment services 713
Open banking 714
Robo-advice 714
Insurance products 715
Credit references 715

CROSS-BORDER REGULATION 716

Passporting 716
Requirement for a local presence 716

SALES AND MARKETING 716

Restrictions 716

CRYPTOASSETS AND TOKENS 717

Distributed ledger technology 717
Cryptoassets 717
Token issuance 718

ARTIFICIAL INTELLIGENCE 719

Artificial intelligence 719

CHANGE OF CONTROL 719

Notification and consent 719

Read this article on Lexology

FINANCIAL CRIME 720
Anti-bribery and anti-money laundering procedures 720
Guidance 720

DATA PROTECTION AND CYBERSECURITY 721
Data protection 721
Cybersecurity 721

OUTSOURCING AND CLOUD COMPUTING 722
Outsourcing 722
Cloud computing 723

INTELLECTUAL PROPERTY RIGHTS 723
IP protection for software 723
IP developed by employees and contractors 724
Joint ownership 725
Trade secrets 725
Branding 726
Remedies for infringement of IP 726

COMPETITION 727
Sector-specific issues 727

TAX 728
Incentives 728
Increased tax burden 728

IMMIGRATION 728
Sector-specific schemes 728

UPDATE AND TRENDS 729
Current developments 729

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

Firms located in the United States have been leaders in fintech innovation. Online securities trading, robo-advisers, peer-to-peer (P2P) payment services, platform lenders, mobile banking and other innovations have existed for decades. With many bank and brokerage firm branches closing, either temporarily or permanently, during the covid-19 pandemic, consumers increased their reliance on online and mobile financial services. The number of trading platforms for digital assets has been increasing, as has the volume of trading. Digital assets have established themselves as an investment class, though the use case for these assets, along with distributed ledger technology, is still evolving.

Notably, the Securities and Exchange Commission (SEC) has in recent months brought a series of enforcement actions against several companies engaged in the blockchain market on the basis that the SEC considers many cryptoassets to be 'securities' for the purpose of

Read this article on Lexology

the federal securities laws. These actions, coupled with additional regulatory and legislative scrutiny of high-profile bank and blockchain firm failures complicates the US regulatory environment for blockchain firms.

In general, the regulatory scheme in the United States is complex, with the jurisdiction of state and federal regulatory agencies frequently overlapping and registration with multiple agencies sometimes required. State and federal agencies have interpreted existing laws to extend their jurisdiction to protect consumers, which can, in some cases, dampen innovation. Initiatives to streamline the licensing requirements in certain areas are being considered.

Finally, a substantial amount of venture capital is available to fund fintech start-ups.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Myriad federal and state regulators provide varying degrees of support to financial innovation, taking the form of:

- temporary exemptions from licensing requirements (regulatory sandboxes);
- alternative disclosure requirements;
- formal declarations stating that a given activity complies with existing law; or
- informal discussions and information-sharing arrangements.

Regulatory sandboxes

Arizona, Florida, Nevada, North Carolina, Utah, West Virginia and Wyoming have all instituted regulatory sandboxes. Financial services providers may apply to the state financial regulator to request exemption from state licensing requirements. Such exemptions are typically limited to a discreet time period. Those admitted to the sandbox must still comply with any applicable consumer protection laws (such as disclosure requirements or interest rate limits) and must agree to share information with the state regulator.

There are no equivalent regulatory sandboxes at the federal level.

Alternative disclosures

The Consumer Financial Protection Bureau (CFPB) has instituted a Trial Disclosure Sandbox in which companies may test for a limited period of time disclosures that financial services providers believe can improve upon existing required disclosures. Companies must share data with the CFPB regarding the effectiveness of the alternative disclosures.

'No-action' determinations

Many federal financial regulators have instituted formal processes through which financial services providers may provide information regarding their products or services and request a determination from the regulator's staff that such offerings will not be subject

to an enforcement action by the regulator for a violation of applicable law. Such 'no-action' relief is not legally binding, but regulators abide by such determinations in practice.

Informal support

The CFPB, the SEC and the Commodity Futures Trading Commission (CFTC) have all formally established offices to interact with fintech companies, provide informal guidance and coordinate with non-US regulators. The offices are not, however, endowed with any formal powers to exempt fintechs from existing requirements. The other federal regulators have not established formal offices, but all offer the opportunity for informal discussions with staff members.

FINANCIAL REGULATION

Regulatory bodies

3 Which bodies regulate the provision of fintech products and services?

	Agency	Regulated entities
Securities	Securities and Exchange Commission (SEC)	Broker-dealers, investment advisers, securities exchanges
	Financial Industry Regulatory Authority	Broker-dealers
	State securities administrators	Broker-dealers, investment advisers
Banking	Office of the Comptroller of the Currency	National banks
	State banking regulators	State banks
	Federal Deposit Insurance Corporation	State banks, national banks
	Federal Reserve Board	State banks that elect to be a member of the Federal Reserve System, bank holding companies
Money transmission	State banking regulators	Peer-to-peer (P2P) payment services, issuers of prepaid cards, cryptocurrency exchanges (in some states), others
	Financial Crimes Enforcement Network (FinCEN)	P2P payment services, Issuers of prepaid cards, cryptocurrency exchanges, others
Non-bank lending	State banking regulators	Non-bank lenders, including non-bank mortgage lenders
	FinCEN	Non-bank mortgage lenders
Consumer protection	Consumer Financial Protection Bureau (CFPB)	Money transmitters, large banks, non-bank lenders, other financial service providers
	Federal Trade Commission (FTC)	Money transmitters, non-bank lenders, other financial service providers

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

Activity	Licensing requirement?	Type of regulated entity
Arranging or bringing about deals in investments that are securities	Yes	Broker-dealer
Making arrangements with a view to transactions in investments that are securities	Yes	Broker-dealer
Dealing in investments that are securities as principal or agent	Yes	Broker-dealer
Advising on investments in securities	Yes	Investment adviser
Lending	Yes	Bank, non-bank lender
Factoring	No	N/A
Invoice discounting	No	N/A
Secondary market loan trading	No	N/A
Deposit-taking	Yes	Bank
Foreign exchange trading	No	N/A
Payment services	Yes	Bank, money transmitter

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

At the federal level, all consumer loans are subject to the Truth in Lending Act (TILA), which requires creditors to provide certain disclosures to consumers regarding the loan, including repayment terms, fees and interest. TILA imposes additional disclosure requirements on credit cards and mortgage loans secured by a consumer's dwelling. TILA imposes substantive restrictions on mortgage loans.

The Secure and Fair Enforcement for Mortgage Licensing Act mandates a nationwide licensing and registration system for companies that make mortgage loans and for individuals working for such companies.

At the state level, non-bank companies that make consumer loans are typically required to obtain lender licences. Licensing requirements vary by state and also by the terms of the loans offered to consumers; loans with higher interest rates are more likely to require the lender to obtain a state licence.

Most states also have usury laws that prohibit lenders from charging interest higher than a specified amount. Usury limits vary by state and by type of loan.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

There are no regulatory restrictions on trading loans in the secondary market in the United States, and trading loans is not subject to direct regulatory authority oversight. Trading or holding some loans may, however, be subject to regulation based on the industry, such as the gaming industry, and the trading of loans in those industries may be subject to governmental or regulatory approvals or other legal and regulatory requirements. Loan market participants such as investment advisers are subject to the Custody Rule under the Investment Advisers Act 1940 (the Advisers Act) with respect to loans.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

An issuer's compliance with applicable laws, rules and regulations will depend on the nature of the issuer's collective investment scheme. Generally, an issuer may have to register a collective investment scheme involving investments in securities under the Investment Company Act of 1940, as amended (the 1940 Act), unless it qualifies for an exemption. Common exemptions from the 1940 Act registration requirements for private funds include sections 3(c)(1) and 3(c)(7), which exempt issuers that have no more than one hundred beneficial owners and whose beneficial securities are owned by qualified purchasers (as defined under the 1940 Act), respectively.

Any person or entity engaged in the business of providing investment advice concerning securities, including those that provide investment advice to collective investment schemes, must consider whether they are required to register with the SEC as a registered investment adviser under the Advisers Act. State investment adviser registration or other regulatory requirements may apply.

An offering of securities, including shares in an investment company, may need to be registered with the SEC under the Securities Act of 1933. Regulation D under the Securities Act provides an exemption from registration requirements if the offering meets certain requirements, including limitations on the number or type of investor.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

In the United States, managers of alternative investment funds that invest in securities are 'investment advisers', and they are regulated by the SEC (under the Investment Advisers Act of 1940) or by state regulators. Managers of commodity pools (namely, funds that invest in commodity interests) are commodity pool operators and commodity trading advisers, which are regulated by the Commodity Futures Trading Commission (CFTC) (under the Commodity Exchange Act).

Read this article on Lexology

Managers will need to register as investment advisers, commodity pool operators or commodity trading advisers, as applicable, unless an exception or exemption is available. Unregistered investment advisers, commodity pool operators and commodity trading advisers are still subject to certain requirements, which may include reporting requirements or notice filings, payment of fees or other requirements.

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

P2P and marketplace lending is regulated at both the federal and state levels. Consumers obtain both types of loans through a fintech provider that connects borrowers and lenders. Loans are either funded by notes sold to investors or by banks, with the loan then purchased by the fintech provider with funds generated by the sale of notes to investors.

Laws that generally apply to all lenders also apply to P2P or marketplace lenders. For the purposes of both federal and state law, a fintech provider may be treated as the 'true lender' even if a bank originated the loan. Additionally, the funding of these loans by investors implicates the securities laws.

At the federal level, applicable lending laws include TILA, the Equal Credit Opportunity Act, privacy laws and advertising and marketing restrictions under the Federal Trade Commission Act.

At the state level, non-bank fintech providers may require a lender licence, and interest rate restrictions will apply and vary by state. As such, certain P2P lenders may be limited in their activities in certain states. Prosper, for example, is not open to residents of Iowa and West Virginia. Meanwhile, residents of Massachusetts and Nevada are ineligible for Happy Money, another P2P lending platform.

Notes sold to investors to fund P2P or marketplace loans are generally securities for purposes of the Securities Act of 1933 and the Securities Exchange Act of 1934. Securities must either be registered with the SEC or be eligible for an exemption. Restrictions on the sales of such securities may also apply.

Crowdfunding

10 Describe any specific regulation of crowdfunding in your jurisdiction.

At the federal level, the SEC regulates equity-based crowdfunding in the United States, including which investors and issuers can participate and how portal operators should conduct business and adhere to reporting requirements. The SEC's Regulation Crowdfunding enables eligible companies to offer and sell securities through crowdfunding. The rules require all transactions under Regulation Crowdfunding to:

- take place online through an SEC-registered intermediary, either a broker-dealer or a funding portal;

- permit a company to raise a maximum aggregate amount of US$5 million through crowdfunding offerings in a 12-month period;
- limit the amount individual non-accredited investors can invest across all crowdfunding offerings in a 12-month period; and
- require disclosure of information in filings with the SEC and to investors and the intermediary facilitating the offering.

Securities purchased in a crowdfunding transaction generally cannot be resold for one year.

Many states have enacted intrastate crowdfunding laws allowing small and emerging companies in these states to raise capital from local, in-state investors through the issuance of securities.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

Invoice trading in the United States is a fairly unregulated industry. Industry associations, including the Secured Finance Network and the American Factoring Association, encourage members to share best practices and provide training and tools to their members. Certain states have recently adopted certain disclosure requirements applicable to invoice trading. For example, in December 2020, SB 5470B, which regulates invoice trading and other alternative forms of financing, was signed into law in New York (this law was amended by SB 898, which was signed into law in February 2021). This law, which became effective on 1 January 2022, imposes disclosure requirements analogous to TILA, on providers of commercial financing in a principal amount of US$2.5 million or less. The law requires disclosure of key transaction terms and the signature of the financing recipient, which may be in electronic form, on all required disclosures before authorising such recipient to proceed with the financing application. A similar law was passed in California in 2018.

Payment services

12 | Are payment services regulated in your jurisdiction?

Payment services and payments services providers are regulated under federal and state law and the rules of private organisations.

Money transmitters, prepaid services providers, money order sellers, and other payment services providers must register with FinCEN and typically must also obtain a licence to operate in each state in which they operate. Each state has separate licensing requirements and there is no multi-state licence.

Electronic payments are subject to the CFPB's Regulation E, which requires certain consumer disclosures and institutes procedures that companies must follow to resolve errors.

The Uniform Commercial Code, as adopted in each state, governs certain non-electronic payment instruments, such as checks.

Read this article on Lexology

The rules of the National Automated Clearing House Association govern transfers using the Automated Clearing House network, a method of electronically transferring funds. The rules of the Visa, MasterCard, and Discover card networks govern transfers using those networks.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

There are no laws or regulations in the United States that require financial institutions to make consumer or product data available to third parties. A consumer may, under US privacy laws, permit financial institutions to share the consumer's data through application programming interfaces (APIs), but the consumer must provide their specific log-in credentials to permit one financial institution to obtain the consumer's data at another financial institution.

In October 2022, the Consumer Financial Protection Bureau proposed a regulatory framework for open banking in the United States, under which covered providers (including financial institutions and card issuers) would be required to provide certain consumer data both to consumers and to authorised third parties. The proposed framework is designed to open consumer data to fintech providers through APIs. This initial proposal is not a notice of proposed rulemaking, and any such notice has yet to be issued.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

The SEC defines a 'robo-adviser' as an automated service with respect to investments in securities that takes in investor information to formulate a 'discretionary asset management service . . . through online algorithmic-based programs'. The sponsors of robo-advisers are required to register with the SEC as investment advisers and, as such, are subject to all of the requirements of the Investment Advisers Act of 1940. The SEC has issued guidance on robo-advisers, as well as investor education information on how robo-adviser platforms work.

SEC guidance has emphasised that robo-advisers should be designed to ensure that methods of gathering information and the types of information acquired are sufficient to meet the fiduciary standards of care and loyalty to which registered investment advisers are subject by considering the best ways to disclose risks and tailor advice to investor needs.

State-registered investment advisers also must consider compliance with any applicable state regulation of robo-advice. Massachusetts, for example, has issued guidance that details required disclosures surrounding the use of robo-advice by its state-registered investment advisers.

Read this article on Lexology

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

Insurers are solely regulated by individual states rather than at the federal level. Fintech insurance does not yet have an individual regulatory framework and is therefore subject to the same regulatory scheme as conventional insurance sales.

Specifically, insurers are subject to licensing requirements in each state in which they operate. Insurers must meet capital requirements as specified by state statute. These requirements vary by state and type of insurance offered (namely, property insurance, life insurance, etc).

Additionally, the majority of states have adopted some version of the Producer Licensing Model Act, which requires a licence if a company is attempting to 'sell', 'solicit' or 'negotiate' insurance. Under these licensing acts, 'sell' is understood to include an exchange of money while 'negotiate' includes selling or obtaining insurance on behalf of another purchaser. 'Solicit' includes attempts to sell, which may include quoting insurance rates and offering product recommendations. Most state licensing acts include exceptions where these activities can be conducted without a licence, such as insurance advertisements, which generally do not constitute solicitation.

It remains unclear whether fintech firms providing automated services for customers, such as automated chatbots offering rates, would trigger solicitation or fall under the advertising exception. The National Association of Insurance Commissioners is currently considering the issue.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

The federal Fair Credit Reporting Act (FCRA) governs consumer reports and consumer reporting agencies. A consumer report is any information bearing on the creditworthiness of a consumer and a consumer reporting agency is any entity that sells such a report. The FCRA requires the following:

- a lender must disclose whether a consumer report has been used to deny credit;
- a consumer reporting agency must disclose to a consumer upon request the information on the consumer's report (often, but not always, free of charge);
- a consumer may dispute any incomplete or inaccurate information;
- consumer reporting agencies must correct or delete incomplete, inaccurate or unverifiable information;
- consumer reporting agencies may not report negative information that is more than seven years old or bankruptcies more than 10 years old; and
- consumers must consent if a consumer report is provided to a current or potential employer.

Read this article on Lexology

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

No. There is no mechanism in the United States for a fintech – or any other entity – that is regulated in a non-US jurisdiction to operate in the United States without the approval of a US regulator if engaged in activities in the United States that subject it to US federal- or state-level regulation. For example, foreign banking organisations may operate branches, agencies, commercial lending companies and representative offices in the United States, but such activities require approval from US state or federal agencies, and are subject to the Federal Reserve Board's Regulation K. Fintech companies that operate as money transmitters or commercial lenders are generally subject to state regulation on money transmission or lending activities made with a jurisdictional nexus to that state (such as, eg, by making loans to residents of the state) regardless of where the fintech company is organised or headquartered.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

Requirements vary from state to state, and a fintech company that engages in regulated activity – deposit-taking, brokerage, investment advice, lending, money transmission or others – will need to examine state law in each jurisdiction they operate in. In some cases, states will require any business that meets certain minimum contact requirements with the state to establish an agent for service of process. In other cases, whether or not a fintech firm operating in a state has a local presence will affect the licensing or registration process, without necessarily meaning that the state requires a physical local presence. To give one example, the California Department of Financial Protection and Innovation requires licensing for certain commercial lenders, including fintech companies that meet the state's licensing criteria. There is a separate licensing application for California-based lenders than for other lenders.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Federal law prohibits financial institutions from engaging in unfair, abusive or deceptive acts or practices (collectively described as UDAAPs). The prohibitions against UDAAPs are applied by the Federal Trade Commission, the Consumer Financial Protection Bureau and the federal banking regulators to financial institutions within their jurisdiction. False or misleading marketing activities may be deemed UDAAPs.

Read this article on Lexology

Financial Industry Regulatory Authority (FINRA) Rule 2210 governs the advertising and marketing practices of broker-dealers. In addition to prohibiting false or misleading public communications, Rule 2210 also requires broker-dealers in certain cases to submit proposed communications to FINRA for pre-approval.

Fintech firms that are registered investment advisers are subject to the advertising and marketing rule (the Marketing Rule) under the Investment Advisers Act. The Marketing Rule regulates advertisements by the registered investment adviser, including testimonials and endorsements from third parties. In general, the Marketing Rule prohibits marketing materials from including untrue statements of material fact or omit material facts in a way that is misleading. Performance results must be presented in a fair and balanced way.

Additionally, Securities and Exchange Commission Rule 10b-5 prohibits fraud or deceit in connection with the purchase or sale of securities. Rule 10b-5 gives the Securities and Exchange Commission broad discretion to deem securities marketing activities unlawful.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

Distributed ledger or blockchain technology is just that: technology. Use of the technology is not subject to financial regulation except when it is used for financial applications, such as evidencing crryptoassets. Blockchain technology has many current applications, and potentially many more in the future, that have nothing to do with financial regulation. For example, blockchain technology can be used as a recordkeeping mechanism, and has been used to keep records of transfers of property, including art and real estate.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

A key question regarding any crryptoasset is whether it constitutes a security. Traditional instruments such as notes, stocks, bonds and other instruments issued for capital raising purposes, including crryptoassets in those forms, are clearly securities. In the United States, the securities laws can also be applied to new or innovative asset classes that meet the definition of a security under the Supreme Court's 1943 Howey test: if there is an investment of money in a common enterprise with the reasonable expectation of profits deriving from the efforts of others, there is an investment contract and therefore a security. In 2019, the Securities and Exchange Commission (SEC) published a Framework for 'Investment Contract' Analysis of Digital Assets, which explains how the SEC applies the Howey test to digital assets. Issuances of digital assets that are securities are subject to the Securities Act of 1933, and secondary market sales of digital assets that are securities are subject to the Securities Exchange Act of 1934.

Read this article on Lexology

The SEC has brought numerous cases in 2022 and 2023 alleging that certain crryptoassets are securities under the Howey test. Notably, the SEC chair has publicly stated on numerous occasions that 'every' token (other than Bitcoin) is a security in his view.

Transfers of digital assets that are not securities through digital exchanges are often deemed 'money transmission' under federal and state law, and the digital exchanges must in many cases register with Financial Crimes Enforcement Network (FinCEN) as a money services business, and in many states become licensed as money transmitters.

Although users of virtual currencies are generally not regulated, they are subject to taxation with respect to the virtual currency they own and sell, which is treated as property under IRS Notice 2014-21, Virtual Currency Guidance.

Additionally, since 2018, federal courts have upheld the authority of the Commodity Futures Trading Commission (CFTC) to apply its anti-fraud authority in the spot market for digital currencies that are commodities, and have found specified virtual currencies to be commodities under the Commodity Exchange Act on a case-by-case basis.

Comprehensive federal regulation of crryptoassets generally, or digital currencies specifically, has not yet materialised. In 2022, a bi-partisan bill was introduced in the Senate by Senators Cynthia Lummis of Wyoming and Kirsten Gillibrand of New York that would, if enacted, impose regulatory requirements on stablecoin issuers, and transfer jurisdiction over most digital assets to the CFTC. A revised version of the bill was expected to be introduced in the Senate in mid-April 2023, however, this has not yet occurred. The bill is unlikely to become law in the near term.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Digital currency exchanges in the United States are required to register as money services businesses with FinCEN and to obtain money transmitter licences in states where their activities constitute money transmission. Certain states, like New York, have established licensing regimes designed to apply to digital currency exchanges or other digital currency businesses, although how well the New York BitLicense works for such businesses is an open question.

Digital currency exchanges are not subject to a comprehensive federal regulatory scheme, though the Chairman of the CFTC has suggested that the US Congress should consider passing legislation establishing one, to increase market confidence in US digital currency exchanges.

Digital assets that are securities must be traded on an exchange that is registered as an alternative trading system (ATS) with the SEC. In 2022, the SEC proposed rules that would expand the reach of Regulation ATS, which received numerous comments from the digital asset industry and cryptocurrency market participants, prompting the SEC to issue a supplemental release reaffirming the application of ATS rules to digital assets.

Read this article on Lexology

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

Both the federal government and the states have enacted legislation regarding artificial intelligence (AI) and have applied their own definitions of the term. However, neither federal nor state-level regulation of AI applies in the financial services industry.

Although no broad system of AI regulation exists in the United States yet, federal and local regulations apply to some of underlying activities that AI is used for. For example, in the financial services industry, sponsors of robo-advisers that use AI to provide investment advice concerning securities to customers are required to register with the Securities and Exchange Commission as investment advisers. In April 2023, four United States agencies, including the Consumer Financial Protection Bureau and the Federal Trade Commission, issued a joint statement indicating that the agencies plan to apply their respective existing enforcement authorities to automated systems, including those that use AI.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

Change in control rules applicable to a regulated fintech entity depends on which regulatory regime applies to that entity. State and federal rules may apply.

At a federal level, for broker-dealers, the applicable self-regulatory organisation, the Financial Industry Regulatory Authority, must approve any change of control. For registered investment advisers, the Investment Advisers Act of 1940 requires that advisory agreements provide for investor consent to a change of control or assignment of an advisory contract.

With respect to state-chartered and national banks, change of control requires filings and approvals under the Bank Holding Company Act, the Change in Bank Control Act and various state laws. The acquisition by a bank holding company of direct or indirect control of more than 5 per cent of the voting shares of a bank requires approval of the Federal Reserve Board, and if any company acquires control of a bank, as the term is defined in the Bank Holding Company Act and regulations thereunder, it becomes a bank holding company subject to the supervision of the Board.

Additionally, the Committee on Foreign Investment in the United States, an interagency group, has the power to review and prevent covered transactions; namely, acquisitions by foreign persons of certain US companies or US real estate that pose or potentially pose national security risks.

Read this article on Lexology

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

The Bank Secrecy Act (BSA), initially adopted in 1970, established the basic framework for anti-money laundering (AML) obligations imposed on financial institutions. Among other things, it authorises the United States Department of the Treasury (the Treasury Department) to issue regulations requiring financial institutions and money services businesses to keep records and file reports on financial transactions that may be useful in investigations and the prosecution of money laundering and other financial crimes. The US Congress has passed other AML laws subsequent to the BSA, including the USA PATRIOT Act, adopted in 2001. The Financial Crimes Enforcement Network (FinCEN), a bureau within the Treasury Department, is the administrator of US AML laws and regulations. The Office of Foreign Assets Control, also a bureau within the Treasury Department, administers US laws governing trade sanctions and terrorist financing.

AML requirements include, inter alia: establishing and following written policies including a customer identification programme, maintaining records of specified transactions, and providing currency transaction reports and suspicious activity reports to FinCEN.

While some fintech firms are not 'covered financial institutions' under the BSA-AML framework, many seek to comply with AML requirements as if they were covered financial institutions. To the extent that the fintech firm partners with a bank, banks may follow their federal banking regulator's guidance regarding managing third-party risk with respect to vendor relationships by requiring such compliance.

State-registered fintech firms are often subject to state laws requiring AML standards, including, for example, digital asset exchanges that operate with the New York BitLicense.

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

FinCEN regularly issues regulatory guidance on AML and preventing financial crime. Some of these items of guidance relate specifically to fintech firms. For example, a 2019 FinCEN advisory discussed risks resulting from abuse of convertible virtual currencies (CVCs). It warned that unregistered entities engaged in CVC businesses present significant risks of illicit finance even when not deliberately attempting to evade supervision. In particular, FinCEN highlighted darknet marketplaces, unregistered peer-to-peer exchangers, unregistered foreign-located money services businesses and CVC kiosks as high-risk businesses, and provided examples of law enforcement action by US authorities against each type of convertible virtual currency business.

Generally applicable FinCEN guidance often includes guidance applicable to fintech firms. For example, a FinCEN alert on evasion of US sanctions against the Russian Federation

in March 2022 warned CVC exchangers and administrators to 'identify and quickly report suspicious activity associated with potential sanctions evasion'.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The Gramm-Leach-Bliley Act (GLBA) governs the privacy and security of data processed and transferred by all financial institutions, including fintechs. The GLBA applies to non-public personal information (NPI) of consumers held by financial institutions. 'Consumers' are individuals who are seeking or have obtained a consumer financial product or service. NPI is personally identifiable financial information that is not publicly available and is comprised of data that can reasonably be linked with a given individual. Aggregated or de-identified data is not NPI and is not subject to the GLBA requirements.

Generally, under GLBA:

- a financial institution may not share NPI with non-affiliated third parties without first providing a consumer with notice and an opportunity to opt out of the sharing;
- a financial institution must provide initial and annual notices to customers describing their privacy policies, including the type of data processed and shared, with whom the financial institution shares NPI, and the financial institution's data security policies; and
- a financial institution must protect the security and confidentiality of NPI.

There are no additional specific restrictions on consumer data transfers from the United States to another country. Consumer data may generally only be transferred from the European Union to a US third party if the US third party agrees to the Standard Contractual Clauses adopted by the European Commission.

Some states, such as California, Colorado, Connecticut, Utah and Virginia, have adopted privacy laws that govern the use of data of those states' residents. However, those state laws typically exempt data that is subject to the GLBA.

There are no additional specific restrictions on consumer data transfers from the United States to another country. Consumer data may generally only be transferred from the European Union to a US third party if the US third party agrees to the Standard Contractual Clauses adopted by the European Commission.

Cybersecurity

28 What cybersecurity regulations or standards apply to fintech businesses?

The GLBA is the primary federal law governing the security of data collected and processed by all financial institutions, including fintechs. The GLBA requires financial institutions to develop a written information security plan (WISP) and:

- designate one or more employees to coordinate the WISP;
- identify and assess the risks to NPI and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards programme, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, including contractual requirements to maintain safeguards, and oversee their handling of NPI; and
- evaluate and adjust the programme as needed.

The Federal Trade Commission revised regulations implementing the GLBA safeguards provisions, which become effective in June 2023. The Securities and Exchange Commission (SEC) has likewise proposed revisions to its Regulation S-P, which implements the GLBA safeguards provisions with respect to SEC registrants, although such revisions have not yet been formally adopted.

Some states have adopted laws governing data security, which generally apply to businesses, including fintechs, with consumers in those states. Massachusetts has adopted the most stringent law, which includes all of the data security requirements of the GLBA listed above, while further imposing specific data security protocols, including encryption of all consumer data at rest or in transit.

Additionally, numerous states have adopted data breach notification laws, which require companies (including fintechs) with consumer data that has been subject to unauthorised access to notify affected individuals and, in some cases, notify the relevant state regulator or chief law enforcement officer.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Legal requirements and regulatory guidance relating to outsourcing of a material aspect of a financial services business depend on the type of financial services business, but in general, federal and state regulators place limits and impose requirements when certain functions are outsourced. These requirements generally provide that the outsourcing of functions to third parties requires oversight of those third parties, and that the financial services firm continues to be responsible for its own compliance with applicable laws.

The federal banking agencies have issued guidance relating to mitigating risks arising from the use of third-party vendors generally. For example, the Federal Reserve Board (FRB) has published SR 13-19, Guidance on Managing Outsourcing Risk, which provides methods for financial institutions to evaluate their contracts with third-party service providers and to mitigate risks related to using such services. Collectively, through the Federal Financial Institutions Examination Council (FFIEC), the federal banking agencies have also issued guidance on outsourcing technology services and on banks' supervision and management

of relationships with technology services providers (TSPs). Such TSPs are often fintech firms providing technology services in coordination with the bank.

With respect to broker-dealers, the Financial Industry Regulatory Authority's NASD Notice to Members 05-48 provides that outsourcing to a third party any function that would require that third party to register as a broker-dealer means that the third party will be treated as an associated person of the broker-dealer, and that broker-dealers are not relieved of responsibility for compliance with legal requirements relating to outsourced services.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

The use of cloud computing by financial services firms raises issues relating to data privacy and data protection, because a cloud computing environment entails a third-party servicer creating information systems for and hosting consumer data on off-site servers.

Federal financial services agencies have published guidance on cloud computing in the financial sector including the FRB's SR 13-19 and the FFIEC Statement on Security in a Cloud Computing Environment (2020) (the FFIEC Statement). SR 13-19 and the FFIEC Statement apply to state-chartered and national banks. With respect to broker-dealers, in 2021 the Financial Industry Regulatory Authority issued a report on 'Cloud Computing in the Securities Industry' that emphasised the importance of cybersecurity, data privacy, business continuity, and third-party vendor risk for firms that employ cloud storage or other cloud-based services.

The use of cloud computing by any financial institution raises issues relating to business continuity in particular. A disruption in service or cyberattack on a cloud-based, third-party network could cause serious problems for a financial institution and its customers. Financial institutions are required to create and maintain business continuity plans and protections for their IT systems. Banks, broker-dealers, and investment advisers are all subject to regulations requiring business continuity plans from their respective federal regulators.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

There are three primary types of intellectual property rights available to protect software: copyright, trade secret and patent.

Copyright

Copyright protects software code in certain circumstances but does not protect the underlying idea or functional expression of software. To be protectable under the copyright laws,

the code must constitute an original work of authorship fixed in a tangible form of expression. Software code is fixed for purposes of copyright protection when it is in a medium that allows it to be perceived either directly or with the aid of a machine or device.

Copyright protection exists from the moment software code is fixed in a tangible form of expression. It is not necessary to register a copyright to obtain copyright protection. Copyright registration does have several benefits, however, including:

- creation of a public record;
- the right to sue for infringement;
- the availability of statutory damages; and
- other benefits.

Registering the copyright in software code requires a completed application form, as well as a filing fee and nonreturnable deposit submitted to the Copyright Office.

Trade secret

Software may be protected as a trade secret provided that the software is kept secret and that the secrecy gives the owner of the software a competitive advantage. Registration is not required to obtain trade secret protection.

Patent

Patent protection may be available for software-implemented inventions or business methods in certain circumstances. Patent rights are obtained through registration.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

Generally, the copyright in a work belongs to the person who created the work. However, when employees have created a work within the scope of their regular employment duties the employer is considered the author and copyright owner of the work unless the parties have agreed otherwise in writing.

In the case of works developed by a contractor or consultant, the hiring party will be considered the author and the copyright owner of the work if:

- the parties expressly agree in a signed written instrument that the work is a 'work made for hire', and
- the work was specially ordered or commissioned for use as one of nine categories of works set out in the copyright code.

In the absence of these criteria, the contractor or consultant is considered the author and copyright owner. Alternatively, contractors and consultants may agree in writing to assign their rights to the hiring party.

Read this article on Lexology

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

Joint owners each have an independent right to use, distribute, copy and grant non-exclusive licences to any work of which they are a joint owner. In the case of copyrights, joint owners have a duty to account to their fellow joint owners for any profits made. A joint owner, however, can only transfer their own rights, not those of another joint owner, and cannot grant an exclusive licence to any third party without the approval of their fellow joint owners. Joint owners are free to change any of these rights by way of written agreement.

Joint owners of a trademark have unlimited rights to use the mark just as if ownership were vested in a single person or entity. However, joint ownership of trademarks is generally discouraged since a trademark is supposed to identify and distinguish a single source of products and services. The law is unsettled as to the extent to which a joint owner of a trademark may assign their entire interest without the approval of their fellow joint owners.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Companies protect their trade secrets by requiring employees, consultants, service providers and business counterparties to enter into non-disclosure agreements preventing the unauthorised use or disclosure of confidential and proprietary information and trade secrets. Employees and consultants also will be required to enter into intellectual property assignment agreements to ensure that the company is the owner of any works created by the individual in connection with their services to the company. Companies will also implement internal controls at their physical work site as well as on their computer networks and company-owned hardware to limit access, use, copying and removal of sensitive materials. Federal and state statutes may provide a private right of action for theft of trade secrets.

During court proceedings, trade secrets may be protected by seeking to limit the scope of discovery, by entering into confidentiality agreements with opposing parties, or by seeking court orders to permit the filing of sensitive materials under seal or to close the courtroom to the public for portions of the legal proceedings. Local rules and statutes will define the parameters a court will consider when deciding whether to seal documents or close the courtroom to the public. Generally, however, a court will balance the public's common-law right of access to judicial proceedings against the trade secret owner's right to maintain the secrecy of its proprietary information in determining whether to grant a litigant's motion to seal court filings or close the courtroom.

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Obtaining a federal trademark registration is one of the best ways to protect branding. A trademark is a word, phrase, symbol, design or other indicia of ownership, or any combination thereof, used to identify and distinguish the source of a product or service. The owner of a trademark can prevent third parties from using the same or a confusingly similar mark to sell the same or related products or services as those of the owner.

In the United States, trademark rights are generally acquired through use of the mark in commerce. However, ownership of a federal trademark registration confers significant advantages over relying on unregistered rights. Among others, these advantages include the following:

- a presumption that the registrant has the exclusive right to use its mark throughout the entire United States;
- presumptions that the registrant owns the mark and that it is valid;
- the registration entitles the owner to file actions concerning the mark in federal court; and
- the registration entitles the owner to enhanced damages if successful in an infringement action.

Registration is obtained by filing an application with the US Patent and Trademark Office.

To avoid infringing existing brands, a trademark search should be conducted prior to adopting a mark or filing an application to see if any identical or confusingly similar brands already exist.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

The remedies available for IP infringement are injunctions, monetary damages – both actual damages and statutory damages – attorney's fees and seizure of the infringing goods. There may also be criminal sanctions for certain violations.

Courts may grant an injunction if a copyright or patent owner establishes that:

- the plaintiff suffered irreparable harm;
- the plaintiff's purported injury outweighs the damage an injunction would inflict on the defendant; and
- an injunction is not counter to public interest.

Once a plaintiff establishes infringement, an injunction can be either temporary or permanent; courts generally grant permanent injunctions where there is evidence of past

infringement and a strong likelihood of future infringements. Additionally, during an infringement proceeding, courts may take into custody any copies or records of the infringing goods as deemed reasonable and can order the destruction or disposition of such goods as part of its final judgment.

A copyright owner is entitled to recover the actual damages suffered as a result of the defendant's infringement plus the defendant's profits attributable to the infringement. Plaintiffs may also elect to seek statutory damages in certain circumstances for infringement of registered works. Copyright owners may seek between US$750 and US$30,000 per work infringed before a final judgment, as determined by the court. Alternatively, if the copyright owner successfully establishes willful infringement, the court may award up to US$150,000 per work at its discretion. If the infringement was not wilfully committed, the court in its discretion may reduce the statutory damages to as little as US$200 per work. Courts may also award reasonable attorney's fees to the prevailing party. If the court determines the infringement was wilful, criminal punishments including fines and prison sentences of up to 10 years may be ordered.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

Competition is an area of regulator focus in the fintech industry. In January 2021, the antitrust division of the Department of Justice (DOJ) reorganised a new unit focused on antitrust enforcement in the financial services sector: the Financial Services, Fintech, and Banking Section. Antitrust scrutiny of the fintech industry by this division is likely to increase going forward, but is already substantial. In 2021, Visa announced the cancellation of its planned acquisition of Plaid, Inc and cited antitrust objections from the DOJ. (Plaid provides a technology platform that allows apps to connect to customer bank accounts through application programming interfaces.)

In October 2021, the Consumer Financial Protection Bureau (CFPB) ordered a number of big tech and social media firms to provide information about their business practices relating to payment systems. The Chair of the Federal Trade Commission (FTC) filed a comment emphasising the FTC's concerns regarding the competitive effects of such business practices. The FTC also submitted a report on privacy and data security to the US Congress in the autumn of 2021 that highlighted its intention to pursue 'competition-based remedies' to consumer protection cases with regard to privacy. In May 2022, the CFPB opened a new unit, the Office of Competition and Innovation, to promote competition and fairness with respect to financial services companies, including fintechs.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

Fintech companies may structure their business in a manner to be eligible for one or more federal income tax incentives. Founders and investors may reduce their tax burdens if they sell stock in a 'qualified small business company'. In addition, R&D tax credits are available for a variety of investments including fintech development.

Certain states have programmes designed to support start-ups (and small businesses) generally but none are specifically geared to the fintech sector, including funding, tax credits, incubator space and partnerships with other businesses, direct government financing, direct and indirect private investment incentives, R&D credits, Small Business Innovation Research and Small Business Technology Transfer Grant Program-related incentives, and sales or use tax and property tax exemptions.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

It is unclear whether any significant tax legislation will be enacted prior to the 2024 US general election cycle.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

The US Department of State overseas a 'first preference' list with respect to immigration into the United States pursuant to employment-related visas. None of the top preferences are specifically related to employees of fintechs as a class. However, there may be many officers and employees of fintech firms who can meet one or more of the preference criteria. The preference levels most likely to be applicable to officers or employees of fintech firms are as follows:

- first preference: 'persons with extraordinary ability' in, among other areas, sciences or business; outstanding professors and researchers and multinational managers or executives of a non-US affiliate of a US employer;
- second preference: professionals holding an advanced degree and 'persons with exceptional ability' in, among other areas, sciences or business; and

- third preference: workers whose jobs require a minimum of two years of training or work experience, or professionals with a baccalaureate degree or its equivalent.

Other immigration categories may apply, depending on the circumstances of a given potential immigrant, including a category for immigrant investors.

UPDATE AND TRENDS

Current developments

41 | Are there any other current developments or emerging trends to note?

Multiple arms of the federal government are currently evaluating legislative or regulatory actions that could impact fintech firms and digital asset firms going forward.

In May 2022, the Federal Reserve Board proposed guidelines that could open a path for non-bank fintechs that have 'novel charters' – such as a Wyoming special purpose bank charter – to obtain master accounts at a Federal Reserve Bank, which would allow the account holder to deposit funds, draw checks against those funds, and have direct access to the Federal Reserve's Payment System Services. However, the Federal Reserve has not approved any Wyoming special purpose bank charter master account applicant.

In October 2022, the Consumer Financial Protection Bureau (CFPB) proposed a framework for allowing access to consumer financial data held by financial institutions, also known as 'open banking', in the United States. This proposed framework is a preliminary step in the CFPB's rulemaking process required by the Small Business Regulatory Enforcement Fairness Act, made prior to a notice of proposed rulemaking, which CFPB expects to be issued sometime in 2023. In November 2022, the CFPB finalised a rule to use a previously unexercised legal provision to examine nonbank financial companies that, in the opinion of the CFPB, pose risks to consumers.

Recent appointees to the Office of the Comptroller of the Currency (OCC), the CFPB and the Securities and Exchange Commission, among other agencies, have changed the approach of these agencies to fintech, including digital assets. The OCC has been silent with respect to its proposed fintech banking charter, signalling that the charter is now moribund, and has been less vocal in its advocacy of digital assets.

The OCC, Federal Deposit Insurance Corporation (FDIC) and Federal Reserve have been more vocal, however, in the insured deposits space following the collapses of Silicon Valley Bank, Signature Bank and First Republic Bank in early 2023. Each financial regulator and various members of the US Congress have promoted theories of blame and of regulatory response to the banking crisis, such as enhanced capital and liquidity requirements and enhanced supervision of financial institutions.

The FDIC has also proposed new obligations for banks and non-bank entities involved in facilitating access to insured deposits. The proposed rule would require insured depository institutions to monitor third parties that provide deposit products, such as broker-dealers

and neobanks, and would require such third parties to revise their disclosures surrounding products that rely on pass-through deposit insurance.

With regard to the digital asset space, the Biden Administration produced the 2023 Economic Report of the President, one chapter of which focuses on digital assets. The Report details the Administration's view that digital assets have delivered few promised benefits of decentralised technologies, such as providing investment opportunities, improving financial inclusion, enhancing payment efficiency and creating value by bypassing traditional intermediaries.

At the agency level, SEC chair Gary Gensler has made a number of statements signalling the SEC's interest in bringing new enforcement actions against digital asset companies, and the SEC's Division of Enforcement has responded in turn by bringing several high-profile cases against crypto-related entities. For example, the SEC has brought an enforcement action against crypto exchange Bittrex and its parent, Bittrex Global, for failing to register as a securities exchange, as well as joining the Commodity Futures Trading Commission (CFTC) and the Department of Justice in bringing actions against Sam Bankman-Fried, the then-CEO of FTX, after the collapse of FTX. In addition, Coinbase has publicly revealed receipt of a Wells notice, generally a precursor to an SEC enforcement action, and distributed Coinbase's lengthy response. Coinbase has also filed a suit against the SEC to force action on a petition of rulemaking on defining securities in the digital asset space.

The Federal Reserve has also been considering digital asset issues, publishing a discussion paper evaluating the pros and cons of a potential central bank digital currency in the United States and issuing a policy statement regarding how the Federal Reserve will interpret its authority to limit the crypto-related activities of state member banks.

There has also been legislation proposed relating to the regulation of digital assets. Several bills have been introduced in the US Congress that would impose regulatory requirements on stablecoin issuers and establish jurisdiction over most digital assets with one of several federal agencies, such as the Federal Reserve or the CFTC. Whether any such bill will become law in the near term is unknown.

* *The authors wish to thankJack Yoskowitz, Daniel Bresler, Daphne Coelho-Adam, Brett Cotler, Joseph Nardello, Richard DiNapoli and Colin Hillfor their assistance in the preparation of this chapter.*

SEWARD & KISSEL LLP

Casey J Jennings	jennings@sewkis.com
Paul T Clark	clark@sewkis.com
Jeffrey M Berman	bermanj@sewkis.com
Beth H Alter	alter@sewkis.com
Seth Kuntz	kuntz@sewkis.com

1 Battery Park Plaza, 23rd Floor, New York NY 10004, United States
Tel: +1 212 574 1200
www.sewkis.com

Read more from this firm on Lexology

Read this article on Lexology

Vietnam

Le Thi Loc, Ha Nguyen Nhat Minh, Ho Ngoc Quynh Anh, Ta Nguyen Nhu Quynh and Ngo Thi Khanh Linh
YKVN

RETURN TO CONTENTS

Summary

FINTECH LANDSCAPE AND INITIATIVES	**733**
General innovation climate	733
Government and regulatory support	734
FINANCIAL REGULATION	**735**
Regulatory bodies	735
Regulated activities	735
Consumer lending	736
Secondary market loan trading	737
Collective investment schemes	737
Alternative investment funds	738
Peer-to-peer and marketplace lending	738
Crowdfunding	739
Invoice trading	739
Payment services	740
Open banking	741
Robo-advice	741
Insurance products	742
Credit references	743
CROSS-BORDER REGULATION	**743**
Passporting	743
Requirement for a local presence	744
SALES AND MARKETING	**744**
Restrictions	744
CRYPTOASSETS AND TOKENS	**745**
Distributed ledger technology	745
Cryptoassets	745
Token issuance	746
ARTIFICIAL INTELLIGENCE	**746**
Artificial intelligence	746
CHANGE OF CONTROL	**746**
Notification and consent	746
FINANCIAL CRIME	**747**

Read this article on Lexology

Anti-bribery and anti-money laundering procedures 747
Guidance 747

DATA PROTECTION AND CYBERSECURITY 748
Data protection 748
Cybersecurity 749

OUTSOURCING AND CLOUD COMPUTING 750
Outsourcing 750
Cloud computing 750

INTELLECTUAL PROPERTY RIGHTS 751
IP protection for software 751
IP developed by employees and contractors 752
Joint ownership 752
Trade secrets 752
Branding 753
Remedies for infringement of IP 753

COMPETITION 754
Sector-specific issues 754

TAX 754
Incentives 754
Increased tax burden 754

IMMIGRATION 755
Sector-specific schemes 755

UPDATE AND TRENDS 755
Current developments 755

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

1 What is the general state of fintech innovation in your jurisdiction?

In Vietnam, fintech is generally defined as the application of innovative, creative, and modern technologies in the banking and finance sector to provide customers with transparent, efficient, and convenient financial services at a lower cost than traditional services systems; accordingly, fintech is classified in the banking and finance sector, which is strictly regulated by the State Bank of Vietnam (SBV). Fintech in Vietnam currently remains nascent in comparison with ASEAN countries (eg, Singapore, Malaysia, Indonesia, the Philippines and Thailand). Only a few fintech segments, such as digital transactions, e-commerce platforms and digital payments (eg, e-wallet, point of sale or payment gateway) are regulated, while most fintech segments are not recognised in Vietnam, such as peer-to-peer (P2P) lending, crowdfunding and blockchain (including but not limited to virtual currencies on the basis of blockchain), because there is no legal framework to govern it. Regardless of the unregulated segment, in practice, some companies are operating in Vietnam by way of registering

Read this article on Lexology

with competent authorities as investment or enterprise management consultancy firms instead of financial institutions.

In general, Vietnam was and is actively looking to grow its fintech sector, and it welcomed potential investors to help the country grow in the area, given that it only possesses mid-level logistics for the fintech sector. The Prime Minister (PM) has instructed relevant authorities to build a testing framework (regulatory sandbox) for financial and banking services based on information technology platforms. SBV has been assigned for drafting a decree on the trial mechanism for the first time in 2020. This draft decree introduced a preliminary trial mechanism that encouraged high-tech companies to participate in the fintech trial mechanism. In April 2022, the second version of the fintech draft decree has been circulated for seeking opinions, which provides certain changes on trial mechanisms for financial technology activities in the banking sector (the Fintech Draft Decree). The Fintech Draft Decree provides fintech segments that fintech companies may be permitted to participate in the trial mechanism, including credit via a technology platform, P2P lending, credit scoring, open application programming interface (Open API), innovative technology application solutions (eg, blockchain, distributed ledger technology) related to banking activities and other technology application supporting banking activities. It is notable that fintech companies cannot engage in unregulated segments unless there is a special pilot approval of the SBV. The timeline for the fintech trial mechanism will not exceed two years.

Government and regulatory support

2 Do government bodies or regulators provide any support specific to financial innovation? If so, what are the key benefits of such support?

Vietnam has not issued any regulations on specific support for financial innovation and has only directed agencies to build a legal framework for fintech, including:

- 2017: Decision No. 328/QD-NHNN of the SBV establishing a fintech steering committee for the purpose of:
    - researching fintech activities, building, and developing a legal framework for fintech; and
    - coordinating with relevant ministries to implement instructions of the PM under Decision No. 844/QD-TTg of the PM on approval for 'Assistance policies on national innovative start-up ecosystem to 2025' in 2016.
- 2019: Decision No. 999/QD-TTg of the PM approving a scheme for the development of a sharing economy to encourage innovation, application of digital technology, and development of digital economy, and implement a trial mechanism for new policies (sandbox) for the development and application of new technologies to the sharing economy model.
- 2020: Decision No. 283/QD-TTg of the PM approving a proposal on services sector restructuring to the year 2020, with an orientation to 2025, which promotes the application of key technologies of the fourth industrial revolution in the management, development, and supply of banking products and services; and building a trial mechanism (regulatory sandbox) for financial and banking services based on information technology such as e-wallets, electronic know your client, peer-to-peer lending and crowdfunding.

Read this article on Lexology

- 2023: Draft amendment of the Law on Credit Institutions assigned to the government to regulate the sandbox mechanism on the application of technology and implementation of new products, services, and business models after being approved by the National Assembly Standing Committee. On 18 May 2023, the Deputy Prime Minister again instructed the SBV to urgently submit the draft decree on the sandbox mechanism for the fintech to the government for promulgation. In June 2023, the SBV promulgated Circular 06/2023/TT-NHNN, which, among others, explicitly permits lending in an online manner and certain requirements on lending via online channels. This adoption creates a legal framework for fintech activities, specifically P2P lending.

Accordingly, the SBV prepared the Fintech Draft Decree providing for the following two types of fintech companies participating in the Six Fintech Segments:

- fintech models and solutions not directly provided by banks; and
- technology solutions applied or supported in banking activities. If the Fintech Draft Decree is adopted, fintech companies can engage in the Six Fintech Segments, which are currently for banking and finance companies only.

In 2021, the PM issued Decision No. 316/QD-TTg approving the pilot implementation of the use of telecommunication accounts for payment of low-value commodities and services (Mobile-Money); pursuant to which, customers can use telecommunication accounts for payment without registration of a bank account.

Based on the results from the trial mechanism, competent authorities will prepare and develop the legal framework for each fintech service and technology.

FINANCIAL REGULATION

Regulatory bodies

3 | Which bodies regulate the provision of fintech products and services?

Currently, there is no single regulatory body responsible for the regulation of fintech products and services. Under the Fintech Draft Decree, the State Bank of Vietnam (SBV) is the sole regulator of fintech products and services that has the authority to issue special pilot approval (Trial Approval). The SBV may seek opinions from different regulatory bodies for approving the sandbox for a specific fintech product or service, such as the National Assembly Standing Committee, the Ministry of Finance (MOF), the Ministry of Industry and Trade and the State Securities Commission (SSC).

Regulated activities

4 | Which activities trigger a licensing requirement in your jurisdiction?

The following activities are regulated and require a licence:

- carrying on securities brokerage;
- carrying on securities investment consultancy;

Read this article on Lexology

- carrying on financial advising relating to securities trading or investment;
- carrying on securities underwriting and sponsorship;
- carrying on proprietary account transactions;
- carrying on securities asset management;
- taking in deposits from the general public;
- handling domestic and foreign settlements and intermediary payment services;
- handling, accepting, and discounting certain types of negotiable instruments;
- underwriting and market-making of government bonds;
- offering and providing discretionary investment management services;
- buying and selling foreign exchange, and acting as an agent for the purchase and sale of foreign exchange;
- carrying on fund management services;
- carrying on fund custodian services;
- carrying on derivative products transactions;
- lending microloans online or offline;
- providing certain types of insurance;
- carrying on credit information services; and
- providing consumer finance services.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Consumer lending is generally regulated by:

- Law on Credit Institutions No. 47/2010/QH12, as amended from time to time (the Law on Credit Institutions);
- Circular No. 39/2016/TT-NHNN prescribing lending transactions of credit institutions or foreign bank branches, or both, with customers (Circular 39) as amended in 2023 by Circular 06/2023/TT-NHNN (Circular 06); and
- Circular No. 43/2016/TT-NHNN, as amended in 2019, prescribing consumer lending by finance companies.

The Law on Credit Institutions provides two types of credit institutions that are allowed to provide consumer lending such as:

- Vietnam-based commercial banks, foreign bank branches and foreign-invested banks; and
- Vietnam-based finance companies.

Both banks and finance companies must obtain an operation licence from the SBV and an enterprise registration certificate from the Department of Planning and Investment. Finance companies are limited to providing loans not exceeding 100 million Vietnamese dong (except for car loans with security). Non-credit institutions such as fintech companies are currently not allowed to provide consumer lending.

Secondary market loan trading

6 Are there restrictions on trading loans in the secondary market in your jurisdiction?

Yes, trading loans in the secondary market in Vietnam are subject to the following restrictions:

- a credit institution (seller) can only sell its bad debts to the Vietnam Asset Management Company (VAMC) and this sale is subject to the supervision by the SBV and the following restrictions:
    - the currency used for the purchase and sale of bad debts is Vietnamese dong (except in the case of special VAMC bonds);
    - all rights and interests associated with the bad debt, collateral and other security measures must be preserved and transferred to the debt buyer under the debt purchase contract;
    - if the VAMC and the credit institution reach an agreement on amending the security conditions of the bad debt, written approval of the borrower and guarantor must be obtained; and
    - the VAMC and credit institutions must report certain information to the SBV;
- an enterprise wholly owned by the state (seller) can sell its bad debts to the Vietnam Debt and Asset Trading Corporation and this sale is subject to approvals of the government and (or) the Prime Minister.
- trading in loans between persons being non-credit institutions or individuals is considered as the assignment of rights to demand the payment of debts or assignment of obligation:
    - for the assignment of the right to demand, the transferor must provide a written notice to the obligor of such assignment, unless otherwise agreed; and
    - for assignment of obligation, the transferor must obtain consent from the obligee; and
    - trading in loans by debt trading companies pursuant to newly issued regulations of the government in 2021 is subject to further guidelines of the government, which have not been issued yet.

Collective investment schemes

7 Describe the regulatory regime for collective investment schemes and whether fintech companies providing alternative finance products or services would fall within its scope.

The establishment and operation of securities investment funds are regulated under Law on Securities No. 54/2019/QH14 (the Law on Securities). Securities investment funds include public funds and member funds, and public funds include open investment funds and closed investment funds. The establishment of public funds must be registered with and approved by the SSC, and the establishment of member funds shall be notified to and approved by the SSC. Only commercial banks, finance companies, finance leasing companies, investment funds, security investment companies and fund managers can receive funding or capital to carry out investment activities based on investment entrustment agreements.

Read this article on Lexology

The peer-to-peer or marketplace lenders or crowdfunding platforms do not fit the definitions of securities investment funds and so are not currently recognised. Currently, there is no specific regulation of fintech companies providing alternative finance products or services under the Law on Securities.

Alternative investment funds

8 Are managers of alternative investment funds regulated?

Managers of alternative investment funds are regulated under the Law on Securities and Law on Credit Institutions. Only commercial banks, finance companies, finance leasing companies, investment funds, security investment companies, and fund managers can receive funding or capital to carry out investment activities based on investment entrustment agreements. In particular, these investment activities are broadly defined as:

- securities investment consultancy conducted by securities companies or securities investment fund managers;
- securities investment fund management conducted by securities investment fund managers;
- securities investment portfolio management conducted by securities investment fund managers; and
- receipt of entrusted funds conducted by credit institutions.

Managers are subject to different regulatory regimes depending on the specific forms of these alternative investment funds; and when fintech regulations are adopted by the government, fintech companies may participate in alternative investment funds (namely, crowdfunding).

Peer-to-peer and marketplace lending

9 Describe any specific regulation of peer-to-peer or marketplace lending in your jurisdiction.

Peer-to-peer (P2P) lending is not regulated under the prevailing laws, and currently, fintech companies are not allowed to engage in P2P lending. In the near future, if the Fintech Draft Decree is adopted, it will permit the fintech companies having obtained Trial Approval to carry out P2P lending. Currently, the Fintech Draft Decree provides certain restrictions for being entitled to a trial mechanism. In particular:

- only a Vietnamese-based company in normal operation that has not registered as a pawn shop service as its business lines are permitted to apply for trial mechanism;
- the legal representative, the director of such company does not have any criminal record and has not been imposed administrative sanction in finance, banking or cybersecurity sectors; and
- the P2P lending solution must be a completely new and unregulated innovative solution and feasible in Vietnam, which brings benefits and added value to service users in Vietnam, especially solutions to support and promote the goal of financial inclusion. This P2P lending solution must be well-developed to manage risks and limit negative impacts on the banking system and banking, be they currency or foreign-exchange

activities. The proposed resolution has been carried out, with full review and evaluation measures in terms of operation and function, use and usefulness.

Given that Circular 06 has adopted the concept of online lending provided by credit institutions, it is expected that the fintech companies engaging in P2P lending to follow similar requirements. Generally, Circular 06 requires online lending must ensure data protection of the banks, customers, loan-related information, e-know-your-customer, having technology and risk management and solutions.

To be selected for the trial mechanism, the company needs to submit an application dossier to the SBV, which will review and examine it. If it is cleared by the SBV, the trial approval will be issued for participation in the trial mechanism.

Crowdfunding

10 | Describe any specific regulation of crowdfunding in your jurisdiction.

Crowdfunding is not regulated or recognised as the legal framework for crowdfunding and is still under development by the SBV. Currently, fintech companies are not allowed to engage in crowdfunding. According to the Fintech Draft Decree, a crowdfunding company can commence operations after complying with the following conditions:

- being selected for the trial mechanism on crowdfunding;
- passing this trial mechanism for a certain period of time decided by the SBV; and
- being subject to some restrictions on the locality of service provision, a number of limited customers and limitation of the services.

To be selected for the trial mechanism, the company needs to submit an application dossier to the SBV, which will review and examine it. If it is cleared by the SBV, the Trial Approval will be issued for participation in the trial mechanism.

Invoice trading

11 | Describe any specific regulation of invoice trading in your jurisdiction.

The Law on Negotiable Instruments and the Law on Credit Institutions provide regulations on debt instruments but are silent on invoice trading.

The Law on Negotiable Instruments applies to categories of negotiable instruments including bills of exchange, promissory notes, cheques and some other negotiable instruments.

The Law on Credit Institutions regulates banking activities that include, among others, factoring. Factoring is a form of credit extension to a goods seller or buyer through acquiring receivable or payable amounts arising from the purchase or sale of goods or provision of services under a contract on goods purchase or sale or service provision while reserving the right to claim these amounts.

Until the government adopts new regulations, invoice trading can only be implemented in the form of factoring by financial institutions, and alternative forms are not allowed.

Read this article on Lexology

Payment services

12 | Are payment services regulated in your jurisdiction?

Non-cash payment (including non-cash payment services and intermediary payment services) is strictly regulated under Decree No. 101/2012/ND-CP (Decree 101) and controlled by the SBV. In particular:

- non-cash payments that can only be provided by Vietnam-based banks:
    - cheques;
    - payment orders;
    - authorised payment orders;
    - collection orders;
    - authorised collection orders;
    - bank cards;
    - letters of credit;
    - monetary remittance via the client's payment account; and
    - receipts and disbursements on behalf of others via the client's payment account; and
- intermediary payment services (IPS) that can be provided by non-credit institutions (IPS provider) include:
    - electronic payment infrastructure provision services: financial switch services, electronic clearing services, and online payment gateway services; and
    - supporting services for payment services: supporting services for authorised collection or payment, e-wallet services, and supporting services for electronic funds transfer;

IPS providers are required to obtain a licence from the SBV. Only Vietnam-based IPS providers can provide the IPS in Vietnam, while offshore IPS providers cannot. There are certain technical, legal, and personnel requirements for the IPS, including a minimum charter capital of 50 billion Vietnamese dong. Further, the IPS is subject to market access restrictions for foreign investors; however, current IPS regulations are silent on the foreign investment restrictions applicable (including foreign ownership limitation). There is no commitment by Vietnam to open this sector to foreign investors under international treaties (eg, Vietnam's commitments to the WTO and Comprehensive and Progressive Agreement for Trans-Pacific Partnership). The competent authorities will decide on any limitations or technical barriers applicable to foreign investors who wish to engage in the IPS. The establishment of a 100 per cent foreign-owned IPS provider is subject to the sole discretion of competent authorities, especially the SBV. Foreign investors hold, directly or indirectly, up to 100 per cent equity interest in a few companies of the total 50 licensed IPS providers published on the SBV website (as of 29 June 2023, 50 IPSs have been licensed).

The SBV has been in the process of amending existing regulations on non-cash payment (including the IPS) since 2019. The SBV's draft decree to replace Decree 101 (the Non-cash Payment Draft Decree) introduces new concepts of e-currency, mobilised currency and pre-paid card. Initially, the SBV proposed a foreign ownership limitation of 49 per cent for the IPS, but this proposal was objected to by experts and IPS providers, and the SBV is

reconsidering it. The Non-cash Payment Draft Decree also provides that certain IPS are not subject to SBV's licence requirement (namely, online payment gateways, supporting services for authorised collection or payment, and supporting services for electronic funds transfer). However, IPS providers will still be required to cooperate with a Vietnam-based commercial bank or a foreign bank branch to conduct the business. Recently, in May 2023, the Deputy Prime Minister instructed the SBV to expedite the submission of the draft of the Non-cash Payment Draft Decree to the Government for official promulgation.

Open banking

13 Are there any laws or regulations introduced to promote competition that require financial institutions to make customer or product data available to third parties?

There are no laws or regulations in Vietnam on open banking. The SBV is considering allowing credit institutions and fintech companies to apply Open API with an Open Canvas solution introduced by NTT. However, the SBV has been working on a draft circular for the legal framework for this application. Under the Law on Credit Institutions, disclosure of data by credit institutions (Vietnam-based banks and finance companies) is heavily restricted. In particular:

- employees, managers and executives of a credit institution (eg, bank and finance company) shall not be permitted to disclose the business secrets of this credit institution (eg, customer and product data);
- credit institutions must ensure confidentiality of information on accounts, deposits, deposited assets and transactions of clients conducted at these credit institutions;
- credit institutions shall not be permitted to provide information to any other organisation or individual about accounts, deposits, deposited assets or transactions of clients conducted at these credit institutions, except when requested by competent authorities or when the client consents; and
- credit institutions shall be permitted to exchange information with each other about their operation.

Robo-advice

14 Describe any specific regulation of robo-advisers or other companies that provide retail customers with automated access to investment products in your jurisdiction.

There is still no regulation on robo-advisers in Vietnam, except for securities segments.

In 2019, the Prime Minister issued Decision No. 242/QD-TTg approving a plan to restructure the securities market and insurance market, which includes assigning the MOF the task of issuing guidelines for the standardisation of activities for opening online accounts and establishing electronic know your client, online-trading, AI asset management and robo-advisory, and digitalising the main assets in the securities market with fintech. In fact, before 2019, robo-advisors on securities segments were implemented by Techcom Securities (namely, TCWealth) and later on by several companies in Vietnam such as MBS Securities (Power Rank) and BIDV Securities (i-Broker and i-Invest).

Read this article on Lexology

Insurance products

15 Do fintech companies that sell or market insurance products in your jurisdiction need to be regulated?

The sale or marketing of insurance products in Vietnam by insurers or non-insurance companies is regulated by the Law on Insurance Business and the Law on Advertising. In particular, a Vietnam-based insurer can sell insurance products via multiple channels including, among others, online or offline. The 2022 Law on Insurance Business currently allows insurers (namely, insurance companies, branches of foreign non-life insurance companies, insurance agents, and insurance brokerage companies) to sell insurance products on the internet. The insurers can, at their discretion, decide on the method of providing insurance products and services online. However, it is not clear whether the insurance products can be sold via an e-commerce platform operated by any other service provider that is not the insurer or not. Thus, the sale or marketing of insurance products through e-commerce platforms may cause the e-commerce platform service providers to fall within:

1 the scope of the insurance agency or insurance broker when providing insurance services and products online; and
2 the scope of the advertising service.

For (1) (insurance agency or insurance broker), these are conditional businesses that fall in the market access restriction list, with restrictions applying to foreign investors; however, there is no foreign ownership limitation for insurance agencies or insurance brokers under Vietnamese law. The licensing authority may, at its sole discretion, seek opinions from the higher-level authorities (eg, the Ministry of Planning and Investment and the MOF) before approving incorporation.

For insurance agency services, in addition to incorporation documents, the company needs to meet the following requirements:

- insurance services and products sold on the Internet must fall within the insurance agent contract scope;
- execution of the insurance agency agreement with the insurer; and
- the staff being Vietnamese citizens, residing locally, having the full civil capacity and holding an insurance agency certificate.

For insurance broker services:

- the company must make their capital contributions in cash (which must not be financed by a loan or investment trust from other entities);
- the managers of the insurance brokerage company must satisfy requirements and qualifications on diplomas, certificates, experience and other conditions as prescribed by the government; and
- undertake that their owner's equity less the minimum legal capital is at least equal to the planned amount of investment in an insurance broker.

In addition, the service providers must set up, maintain and operate their information technology systems for such insurance products distribution channels. Other than the

application of information technology in providing insurance services and products, information technology is applied in insurance business activities for a number of purposes (namely, improving the efficiency of the insurance business and modernising statistics and reporting).

For (2) (advertising services), the display of the insurance products on the platform (such as the introduction of products) is regarded as aimed at the public for introducing the insurers and their products and services. Hence, this display would be considered an advertising activity under the Law on Advertising and Vietnam's Commitments to the World Trade Organization; and a foreign-invested company engaging in advertising services is required to have a local partner who has registered a business line of advertising.

Credit references

16 Are there any restrictions on providing credit references or credit information services in your jurisdiction?

Currently, there are two organisations providing credit information services: the Credit Information Centre under the SBV and a company named Vietnam Credit Information Joint Stock Company, which is owned mostly by Vietnam-based banks, which have been licensed by the SBV to provide credit information services.

Credit information services are regulated by Decree No. 58/2021. 'Credit information' is data and relevant data of borrowers and clients at participating institutions, including credit institutions, foreign bank branches, non-credit institutions, and foreign bank branches that provide property rental services, instalment purchase services, pawn shop services under conditions of interest, duration, rental and security interest under law.

In addition to incorporation documents, a credit information company must obtain a certificate of eligibility issued by the SBV to provide credit information services and satisfy the following conditions, among others, technical facilities, personnel, the minimum charter capital of 30 billion Vietnamese dong and agreements with at least 15 participating institutions being Vietnam-based banks and foreign bank branches that agree to provide credit information to only a credit information company. The credit information company shall only receive credit information from the participating institutions if the concerned borrowers give consent to the information collection. We are not aware of any other credit information service provider that has obtained this SBV approval.

CROSS-BORDER REGULATION

Passporting

17 Can regulated activities be passported into your jurisdiction?

Regulated activities cannot be passported into Vietnam, except for the following cross-border banking and finance activities:

insurance:

- insurance services provided to foreign-invested enterprises and foreigners working in Vietnam;
- reinsurance services;
- insurance services relating to international maritime transport and international commercial aviation, and goods in international transit;
- insurance broking and reinsurance broking services; and
- consultancy, actuarial, risk assessment and claim settlement services; and
- banking and finance:
- provision and transfer of financial information and financial data processing and related software by suppliers of other financial services; and
- advisory, intermediation and other auxiliary financial services provision.

In addition, the Non-cash Payment Draft, which would replace Decree No. 101/2012/ND-CP, introduces a new concept of a foreign payment service provider, which is a foreign company:

- entitled to provide payment services according to foreign law, including banks, international card organisations, switching organisations and payment intermediaries, etc; and
- cooperating with a Vietnam-based bank or licensed intermediary payment services.

Requirement for a local presence

18 Can fintech companies obtain a licence to provide financial services in your jurisdiction without establishing a local presence?

For the six segments of fintech services in the Fintech Draft Decree, only local legal entities can obtain licences. For the remaining fintech services, there is no legal framework, so onshore or offshore provision of services is not permitted.

SALES AND MARKETING

Restrictions

19 What restrictions apply to the sales and marketing of financial services and products in your jurisdiction?

Restrictions on the sale and marketing of financial services and products in Vietnam are provided by various legal documents and authorities, depending on the types of services and products.

Insurance companies must be established and obtain a licence from the Ministry of Finance (MOF) to sell their insurance products. In addition, the insurance companies must obtain the MOF's approval before they can sell life and health insurance products. For non-life insurance products (except for vehicle insurance), only the rules, terms and premium scales must be registered with the MOF. The insurance agents are prohibited from:

- providing false information and advertisements about insurance services and the scope of business of insurance companies and mutuals providing microinsurance products; and

- providing insurance terms and conditions prejudicing legitimate rights and interests of policyholders (among others).

insurance brokerage companies are prohibited from providing false information or information irrelevant to insurance requirements, terms and conditions imposed by insurance companies (among others).

Securities companies, securities investment fund management companies and branches of foreign securities companies and fund management companies are not allowed to provide statements or guarantees to clients about the level of income or profit obtainable from investments of the clients and cannot guarantee that clients will not suffer losses (except for fixed revenue securities).

Persons other than credit institutions are prohibited from conducting banking activities (including deposit-taking services, credit extension services and payment services via accounts), except the escrow, purchase and sale of securities by securities companies. intermediary payment services (IPS) providers can only provide the IPS according to their IPS licence.

CRYPTOASSETS AND TOKENS

Distributed ledger technology

20 Are there rules or regulations governing the use of distributed ledger technology or blockchains?

Under Decree No. 101/2012/ND-CP, any payment method that has not been approved by the State Bank of Vietnam (SBV) is prohibited. Distributed ledger technology or blockchain may fall into non-cash payment, which needs the SBV's approval. Currently, there are no specific rules or regulations governing the use of distributed ledger technology or blockchain. Thus, the use of distributed ledger technology or blockchain in the banking and financial sector in Vietnam is not yet recognised. However, in 2021, the Prime Minister promulgated Decision No. 942/QD-TTg, by which the SBV is assigned to study, develop and test for the use of digital currency on the basis of blockchain. The SBV has included blockchain and distributed ledger technology (DLT) as one of the six fintech segments in the Fintech Draft Decree.

Cryptoassets

21 Are there rules or regulations governing the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and non-fungible tokens (NFTs)?

Digital wallets are governed by Decree No. 101/2012/ND-CP (Decree 101), and licensed intermediary payment service providers can provide digital wallets. Cryptoassets have not been recognised in Vietnam. In particular, only non-cash payments provided in Decree 101 and other payment methods approved by the SBV are permissible under Vietnamese law; otherwise, they are prohibited. In 2017, the SBV, through its Official Letter No. 5747/NHNN-PC, firmly stated that digital currency is prohibited in Vietnam. The Non-cash Payment Draft

Decree, which would replace Decree 101, introduces new concepts of e-currency, mobilised currency and pre-paid card.

Token issuance

22 Are there rules or regulations governing the issuance of tokens, including security token offerings (STOs), initial coin offerings (ICOs) and other token generation events?

Virtual currency trading is generally prohibited in Vietnam, and digital currency exchanges and brokerages are also banned. In addition, credit institutions must inform the competent authorities if they are aware of any suspicious transactions relating to virtual currency.

ICOs are not considered securities under Vietnamese law and thus, ICOs or token generation events are not recognised in Vietnam. In 2018, the State Securities Commission under the MOF responded to a Vietnam-based company that the current legal framework does not allow fundraising by the issuance of virtual currencies and such a company should not carry out any activities relating to this fundraising.

ARTIFICIAL INTELLIGENCE

Artificial intelligence

23 Are there rules or regulations governing the use of artificial intelligence, including in relation to robo-advice?

In 2021, the Prime Minister (PM) issued Decision 127/QD-TTg promulgating a national strategy on research, development, and application of artificial intelligence up to 2030, which assigns various ministries' goals and targets on artificial intelligence-related computer programs. The Ministry of Science and Technology is the key ministry coordinating with the relevant ministries and will report on them to the PM. However, there is still no regulation on artificial intelligence in Vietnam as well as draft regulations on the same.

CHANGE OF CONTROL

Notification and consent

24 Describe any rules relating to notification or consent requirements if a regulated business changes control.

In 2017, the State Bank of Vietnam, through Official Letter No. 8104/NHNN-TT, requested all intermediary payment services (IPS) providers to notify of any change of their owners. The Non-cash Payment Draft Decree, which would replace Decree No. 101/2012/ND-CP, adds a time limit of notification within 30 days of any change on owners, charter capital or ownership ratios of IPS providers.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

25 Are fintech companies required by law or regulation to have procedures to combat bribery or money laundering?

Yes. The Law on the Prevention of Money Laundering applies to non-financial institutions engaged in fintech service and payment services, among other things. The Department of Anti-Money Laundering under the State Bank of Vietnam (SBV) monitors and regulates Vietnam's anti-money laundering regime. The Anti-Money Laundering Law (AML Law) mandates that all financial institutions involved in specific business activities (referred to as 'reporting entities') must implement measures against money laundering, and they must also comply with other requirements as required by the AML Law. In particular, the reporting entities are required to comply with the statutory obligations set forth in the AML Law, including, among others:

- reporting certain transactions to the competent authorities, including high-value transactions, suspicious transactions, and transactions involving companies or individuals in the countries and territories on the 'black list' published by the Financial Action Task Force (an inter-governmental body setting standards and promoting effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system);
- conducting know-your-client procedures (eg, gathering, updating and verifying customer identification information);
- conducting an enhanced due diligence investigation on high-risk parties, which include foreign individuals on the list of 'politically influenced persons' published by the SBV to produce a list of their customers or individuals who fall into this category;
- establishing policies and procedures to identify and assess customers' money laundering risk levels before providing new products and services; or services and products using new technologies; and
- performing an enhanced due-diligence investigation on high-risk parties, including foreign individuals on the list of 'politically influenced persons' and persons conducting transactions using new technologies (eg, technology enabling remote transactions).

Guidance

26 Is there regulatory or industry anti-financial crime guidance for fintech companies?

Payment transactions involving digital assets or cryptocurrency between credit institutions are prohibited under current laws.

In 2018, the Prime Minister (PM) issued Directive No. 10/CT-TTg on the management and control of virtual currency in Vietnam, pursuant to which, the PM prohibits trading or use of virtual currency. Following which, the SBV also issued Directive No. 02/CT-NNHH, which bans credit institutions and payment service providers from becoming involved with or providing any services that may transfer, trade, or exchange virtual currency. In addition,

they must inform the competent authorities when aware of any suspicious transactions relating to virtual currency.

In 2021, the SBV issued Directive No. 02/CT-NHNN requiring all credit institutions (including banks, non-bank credit institutions, microfinance institution, and people's credit funds) and intermediary payment services providers to check and apply appropriate methods to control risks of money laundering, terrorist sponsorship and tax evasion during the performance of payment services, card payment services or any payment relating to illegal acts, gambling and virtual currency transactions.

DATA PROTECTION AND CYBERSECURITY

Data protection

27 What rules and regulations govern the processing and transfer (domestic and cross-border) of data relating to fintech products and services?

The Law on Cyberinformation Safety: sets out the main requirements and principles on, among other things, data protection in cyberspace for all entities, including fintech companies. Its key principles on data protection relating to data protection include:

- collecting personal information if consented to in advance by the owner on scope, for the purpose of collection and use;
- using collected information for the purposes consented to by the owner, and only use for other purposes if agreed to by the owner;
- not transferring, sharing or publishing collected information, unless agreed to by the owner or requested by competent authorities;
- any organisation engaging in processing personal information is responsible for the protection of such data; and
- applying necessary measures for data protection.

Personal information must be kept confidential, and any transfer or disclosure must be consented to in advance.

The Law on Cybersecurity: requires overseas and local companies that:

- are providing services on telecommunication networks, the internet, and other value-added services in cyberspace in Vietnam, (namely, cyberspace service providers); and
- are involved in the collection, exploitation, analysis, and processing of personal information, users' relationships and data generated by users in Vietnam to store personal data within the territory of Vietnam for a period specified by the government.

Recently, the government has promulgated Decree No. 13/2023/ND-CP on personal data protection (Decree 13), which comes into force on 1 July 2023, and is considered to be a unified set of regulations on personal data protection. This Decree still requires broader implementation and there is expected to be a period of uncertainty until detailed guidance is provided. Generally, any person or organisation collecting or processing personal information is obligated to notify the data subjects on, among others, its purposes for processing

such data, processing methods, unexpected consequences or damages that are likely to occur from the processing of their personal information, and specific timing for the data processing. Any collection, publication, processing, transfer to a third party or any other use of a data subject's personal information requires the prior consent of such data subject. Such consent must be clearly and specifically expressed, such as in writing, by voice, by ticking of a consent box, etc, and must be verifiable.

Under Decree 13, the scope of the cross-border transfer of personal data includes:

- the use of cyberspace, electronic means or equipment, or other forms to transfer personal data of Vietnamese citizens to a location outside Vietnam's territory; or
- the use of a location outside Vietnam's territory for processing of personal data of Vietnamese citizens.

The cross-border transfer of personal data must satisfy some specific requirements, including:

- obtaining the data subject's consent for the cross-border transfer of personal data;
- preparing, maintaining, and submitting the cross-border transfer impact assessment dossier for inspection and appraisal by the Ministry of Public Security; and
- submitting written notification to the Department of Cyber Security and Hi-Tech Crime Prevention of the Ministry of Public Security upon the completion of the transfer of personal data.

Cybersecurity

28 | What cybersecurity regulations or standards apply to fintech businesses?

There is no specific regulation on cybersecurity related to fintech business. The Law on Cybersecurity applies to all sectors involved in cyberspace, including the fintech sector. In particular, personal information collected, analysed or processed by either domestic or foreign enterprises providing services in the telecommunications network, the internet, and value-added services in cyberspace in Vietnam must be stored in Vietnam. In addition, the personal information of users must be protected.

In addition, the Law on Cybersecurity prohibits the use of cyberspace (by anyone) to conduct the following acts:

- using cyberspace, IT and electronic media to breach laws on national security, social order and safety;
- organising, activating, colluding, instigating, bribing or cheating or tricking, manipulating, training or drilling people to oppose Vietnam;
- distorting history, denying revolutionary achievements, destroying the national solidarity block or conducting offences against religion, gender discrimination or racist acts;
- providing false information, causing confusion among citizens, causing harm to socio-economic activities, causing difficulties for the operation of state agencies or of people performing public duties or infringing the lawful rights and interests of other agencies, organisations and individuals;
- providing or introducing activities being prostitution, social evils or human trafficking;

- publishing information that is lewd, depraved or criminal;
- destroying the fine traditions and customs of the people, social ethics or the health of the community; and
- inciting, enticing or activating other people to commit crime.

Other than the Law on Cybersecurity, Decree 13 also provides a number of principles for protecting data, including:

- the personal data is processed in accordance with the law;
- the personal data subject must be aware of their activities relating to the process of their personal data;
- the personal data must be processed for the purpose limitation;
- the collected personal data must be suitable and limited within the scope of the processing purposes;
- the updated and supplemented personal data must be complied with the processing purposes;
- personal data is subject to protection and security measures during processing;
- personal data is only stored for a period suitable for the purposes of data processing; and
- the fintech companies are responsible for complying with the data handling principles.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

29 Are there legal requirements or regulatory guidance with respect to the outsourcing by a financial services company of a material aspect of its business?

Credit institutions (including foreign bank branches) must ensure safety and confidentiality in e-banking operations under the State Bank of Vietnam's guidance and the provisions of the law on e-transactions. Credit institutions can lease technical infrastructure from third parties and must be responsible for performing e-transactions through these facilities, including preserving the confidentiality of personal information and information of enterprises and organisations, ensuring the security of information systems, participating in response to incidents and taking remedial actions in accordance with the law.

Cloud computing

30 Are there legal requirements or regulatory guidance with respect to the use of cloud computing in the financial services industry?

Cloud computing service in banking operations means the delivery of computer system resources (including computing, networks, storage and software applications and other computer system resources) through a network environment that enables ubiquitous users to access, adjust and pay according to user demand.

Institutions using cloud computing services must:

- carry out an assessment of information technology risks and operating risks;
- classify activities and professional operations expected to be performed on cloud computing based on the assessment of impacts;
- develop backup plans for components of information systems of level 3 or higher;
- establish criteria for the selection of third parties providing cloud computing services; and
- review, amend and apply information security methods, and limit access through cloud computing to its information systems.

Third parties providing cloud computing services must:

- be enterprises; and
- own information technology infrastructure corresponding to the service requested by the institution, which must:

    - comply with the laws of Vietnam; and
    - have been granted a valid international certificate of information security.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

31 Which intellectual property rights are available to protect software, and how do you obtain those rights?

Software can be deemed as a computer program, which means a set of instructions expressed in the form of commands, codes, diagrams and other forms that, when incorporated in a device or equipment operating by a computer programming language, are capable of enabling the computer or the equipment to perform a job or achieve a specific result in accordance with Law on Intellectual Property No. 50/2005/QH11 as amended in 2009, 2019 and 2022 (the IP Law). Accordingly, the software can be protected under copyright, irrespective of whether the software is expressed in the form of source codes or machine codes.

Copyright of software includes moral rights (namely, the right to give titles, the right to attach real names or pseudonyms, the right to publish or authorise to the public, and the right to protect the integrity) and economic rights (namely, the right to make derivative, display, reproduce, distribute, communicate and lease works). The rights holder can make registration to the Office of Intellectual Property to protect their intellectual property right. Copyrights of works arise from the time the specific work is created and expressed in a certain material form, regardless of the content, quality, form, medium or language, whether it is published or unpublished, or whether it is registered or unregistered.

IP developed by employees and contractors

32 Who owns new intellectual property developed by an employee during the course of employment? Do the same rules apply to new intellectual property developed by contractors or consultants?

The owner of IP rights over a particular work and the author of this work is not necessarily the same. Under the IP Law, unless otherwise agreed:

- for copyright (including computer programs), any entity that assigns the task to an employee, contractor or consultant for the creation of a work shall be considered as the owner of copyright with respect to this work; and
- for other industrial property rights (namely, patent, industrial design, and layout design), any entity that provides funding and facilities to the author through the task assignment or employment shall be considered the owner of the industrial property rights.

If the copyright owner over a particular product is not also the author of this work, the owner is entitled to:

- all the economic rights pertaining to this work; and
- only the moral right to publish his or her works or to authorise other persons to publish his or her works.

The authors and the owner of IP rights for computer programs can agree in writing on repairing and upgrading computer programs.

Joint ownership

33 Are there any restrictions on a joint owner of intellectual property's right to use, license, charge or assign its right in intellectual property?

The author retains moral rights. Joint owners are not restricted from using, licensing, charging, or assigning if both agree to do so.

Trade secrets

34 How are trade secrets protected? Are trade secrets kept confidential during court proceedings?

Trade secrets are protected under industrial property rights. Industrial property rights to a trade secret are established on the basis of lawfully obtaining a trade secret and keeping it confidential. Thus, industrial property rights to trade secrets are established without the need for registration with the competent authority. However, protection requires the following conditions:

- it is neither common knowledge nor easily obtainable;
- when used in business activities, it will create for its holder advantages over those who do not hold or use it; and

- the owner of the trade secret maintains its secrecy by necessary means so that it will neither be disclosed nor be easily accessible litigation authorities and officers must keep professional secrets, trade secrets and personal secrets of the involved parties pursuant to their legitimate petitions

Branding

35 What intellectual property rights are available to protect branding and how do you obtain those rights? How can fintech businesses ensure they do not infringe existing brands?

Branding may not be protected if it stands independently, but it is protected as trademarks or trade names.

Industrial property rights to trademarks shall be granted based on decisions issued by competent authorities in accordance with registration procedures specified in the IP Law or on the basis of international registration granted in accordance with the international agreement to which Vietnam is a signatory. Industrial property rights to well-known trademarks shall be granted based on their use instead of registration. The trademark search is an important step in the process of industrial property protection registration to avoid the situation that the trademark application is returned due to duplicate or misleading issues.

Industrial property rights to a trade name shall be established on the basis of lawful use thereof.

Remedies for infringement of IP

36 What remedies are available to individuals or companies whose intellectual property rights have been infringed?

Any intellectual property rights holder shall have the right to apply the following measures for protection:

- to apply technological measures to prevent acts of infringement including:
    - giving instructional information that the product is the subject of intellectual property rights and to warn others not to infringe; and
    - using means or technical measures to mark, identify, distinguish and protect the protected product; and
- to request any infringing party to terminate such act, to remove and delete infringing content on the telecommunications network and the Internet, to make a public apology or rectification, and pay damages;
- to request the competent state body to deal with acts of infringement in accordance with the law; and
- to initiate a lawsuit at a court or a claim at an arbitration centre.

COMPETITION

Sector-specific issues

37 Are there any specific competition issues that exist with respect to fintech companies in your jurisdiction?

The competition laws apply generally to all forms of businesses.

TAX

Incentives

38 Are there any tax incentives available for fintech companies and investors to encourage innovation and investment in the fintech sector in your jurisdiction?

The Investment Law provides investment incentives such as lower corporate income tax rate for certain periods (eg, 10 per cent corporate income tax for 15 years), exemption from import tax, exemption from land fees and land rent, and accelerated depreciation applicable to:

- start-up projects, national innovation centres, and research and development centres; and
- high-tech enterprises and projects involving high technology that are prioritised for investment (eg, blockchain, cloud computing, big data technology and analytics, and artificial intelligence).

Fintech can fall into either of the two categories, depending on the conditions of the actual project.

Increased tax burden

39 Are there any new or proposed tax laws or guidance that could significantly increase tax or administrative costs for fintech companies in your jurisdiction?

There is no new or proposed tax law or guidance that could significantly increase tax or administrative costs for fintech companies in Vietnam. There is no new specific tax law relating to fintech.

IMMIGRATION

Sector-specific schemes

40 What immigration schemes are available for fintech businesses to recruit skilled staff from abroad? Are there any special regimes specific to the technology or financial sectors?

There are no immigration regimes specifically for fintech talent. Enterprises, organisations, individuals and contractors must only employ foreigners to hold positions of managers, executive directors, specialists and technical workers when the professional requirements for which cannot be met by Vietnamese workers.

UPDATE AND TRENDS

Current developments

41 Are there any other current developments or emerging trends to note?

Vietnam is still a country where fintech regulations are relatively new and vague. The prospect of a regulatory sandbox has attracted many new players; however, given the difficulties in obtaining licences, many have opted to acquire existing licensed intermediary payment service providers to build out their services.

YKVN
HANOI • HO CHI MINH • SINGAPORE

Le Thi Loc	loc.le@ykvn-law.com
Ha Nguyen Nhat Minh	minh.ha@ykvn-law.com
Ho Ngoc Quynh Anh	anh.ho@ykvn-law.com
Ta Nguyen Nhu Quynh	quynh.ta@ykvn-law.com
Ngo Thi Khanh Linh	linh.ngo@ykvn-law.com

Suite 1102 The Metropolitan, 235 Dong Khoi Street,
District 1, Ho Chi Minh City, Vietnam
Tel: +84 28 3822 3155
www.ykvn-law.com

Read more from this firm on Lexology

Read this article on Lexology

MORE TOPICS AVAILABLE ONLINE AT LEXOLOGY.COM/GTDT

Including

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements