FINTECH 2023

Contributing editors
Angus McLean and Oliver Irons
Simmons & Simmons LLP

LEXOLOGY
Getting the Deal Through

simmons+simmons

simmons +simmons

Our fintech team delivers legal and commercial advice for a wide range of businesses from fast-growing start-ups to some of the world's largest companies.

The Simmons team has been immersed in the fintech ecosystem since 2014 – a lifetime by the standards of this rapidly-evolving sector. We have extensive knowledge of the sector and an established network allowing us to support our clients beyond the realms of traditional legal advice.

Working with organisations across a broad range of verticals including crypto assets, payments, distributed ledger technology, digital banking, crowdfunding, wealthtech, insurtech and regtech – we help our clients address a wide range of legal challenges. For start-up and scale-up businesses we advise on regulation, tax, employment, incentives, IP, structuring, corporate governance and investment – supporting many towards unicorn status. For our global institutional clients, we advise on areas such as product development, commercial agreements, partnerships, investments and M&A.

Our understanding of the base technology underpinning fintech solutions combined with our knowledge of financial regulation sets us apart. It means our clients, regulators, and policy makers want to work closely with us. We have lawyers on the ground in key fintech hubs, including Hong Kong, Singapore, the UAE and the UK.

simmons-simmons.com

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Head of business development
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Holborn Gate, 330 High Holborn, London,
WC1V 7QT, UK

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between July and August 2022. Be advised that this is a developing area.

© Law Business Research Ltd 2022
No photocopying without a CLA licence.
First published 2016
Seventh edition
ISBN 978-1-83862-539-9

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

FINTECH 2023

Contributing editors
Angus McLean and Oliver Irons
Simmons & Simmons LLP

Lexology Getting the Deal Through is delighted to publish the seventh edition of *Fintech*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting the Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes a new chapter on South Korea.

Lexology Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Angus McLean and Oliver Irons, for their continued assistance with this volume.

LEXOLOGY
Getting the Deal Through

London
August 2022

Contents

Introduction 5
Angus McLean and Oliver Irons
Simmons & Simmons LLP

Belgium 6
Dimitri Van Uytvanck, Jérémie Doornaert, Martin Carlier and Mathieu Vancaillie Simmons & Simmons
Marc De Munter Baker Tilly

Canada 18
Alix d'Anglejan-Chatillon, Ramandeep Grewal, David Elder, Shawn Smith and Éric Lévesque
Stikeman Elliott LLP

China 27
Jingyuan Shi, Yuchen Lai and Yanyu Lai
Simmons & Simmons

Denmark 37
Rasmus Mandøe Jensen and Jónas Már Torfason
Plesner Advokatpartnerselskab

Egypt 46
Mohamed Hashish and Farida Rezk
Soliman, Hashish & Partners

France 53
Hubert de Vauplane and Judith Smadja
Kramer Levin Naftalis & Frankel LLP

Germany 64
Christopher Götz, Elmar Weinand, Felix Biedermann, Jochen Kindermann, Martin Gramsch, Sascha Kuhn and Lena Menger
Simmons & Simmons

Hong Kong 76
Donia Chu, Jolyon Ellwood-Russell, Michelle Ta and Ian Wood
Simmons & Simmons

Indonesia 85
Winnie Yamashita Rolindrawan and Ruth Margaretha Ginting
SSEK Legal Consultants

Ireland 93
Joe Beashel and Ian O'Mara
Matheson

Japan 101
Ken Kawai, Akihito Miyake, Tomoyuki Tanaka, Yutaka Shimoo and Kensuke Inoue
Anderson Mōri & Tomotsune

Luxembourg 109
Cathrine Foldberg Møller, Julie Carbiener, Camille Saettel, Nessym Tir and Camille Bénézet
Simmons & Simmons

Malta 118
Leonard Bonello and James Debono
Ganado Advocates

Netherlands 126
Koen van Leeuwen, Jeroen Bos, Meike Hoekstra and Marise Kok
Simmons & Simmons

Nigeria 138
Ugochukwu Obi, Tare Olorogun, Omolade Afonja, Philips Adekemi and Anthony Obidike
Perchstone & Graeys

Singapore 145
Yingyu Wang and Ashleigh Low
Simmons & Simmons

South Korea 155
Juho Yoon, Young Ju Park, Se Young Im and Jinhee Rhew
Bae, Kim & Lee LLC

Spain 163
Alfredo de Lorenzo, Álvaro Muñoz, Carmen Torres, Ignacio González, Juan Sosa, María Tomillo and Raquel Ballesteros
Simmons & Simmons

Sweden 175
Emma Stuart-Beck, Nicklas Thorgerzon, Caroline Krassén and Anton Sjökvist
Vinge

Switzerland 184
Luca Dal Molin, Daniel Haeberli, Stefan Oesterhelt, Richard Stäuber, Manuel Baschung and Alexander Wherlock
Homburger

Taiwan 194
Abe T S Sung and Eddie Hsiung
Lee and Li Attorneys at Law

Turkey **204**
Cigdem Ayozger Ongun and Deniz Erkan
SRP Legal

United Arab Emirates **217**
Raza Rizvi and Muneer Khan
Simmons & Simmons

United Kingdom **230**
Angus McLean, Oliver Irons, David Trapp, George Morris, Jo Crookshank, Kate Cofman, Minesh Tanna and Olly Jones
Simmons & Simmons

United States **248**
Paul T Clark, Jeffrey M Berman, Beth H Alter, Casey J Jennings and Jessica Cohn
Seward & Kissel LLP

Vietnam **259**
Le Thi Loc, Nguyen Duy Duong, Ta Nguyen Nhu Quynh and Ho Ngoc Quynh Anh
YKVN

Introduction

Angus McLean and Oliver Irons

Simmons & Simmons LLP

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, 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. There can never have been a better 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 saving;
- 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 CDBCs

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 12 to 18 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 potentially even cause systemic risks to the financial system. This has caused a marked shift in the attitude of many policymakers and regulators to the level of support afforded to, and their oversight of, fintech companies. In no area is this more apparent than the world of cryptoassets, where regulators around the globe are grappling with how best to regulate the ever-expanding mosaic of businesses operating in the cryptoassets space. Ironically, this tightening of the regulatory perimeter around cryptoassets, coincides with a marked uptick in the level of activity around the world, from governments and central banks, investigating how they can leverage the same distributed ledger technology to launch their own central bank digital currencies (CDBCs), or revamp their wholesale payments systems. The Bank of International Settlements (often referred to as the central bank of central banks) reported in June 2022 that nine out of 10 of the central banks it surveyed around the world confirmed that they were exploring the use of CDBCs.

However, cryptoassets firms are by no means the only fintech companies experiencing regulatory headwinds. Companies providing buy now, pay later credit products to consumers are increasingly under the spotlight in many jurisdictions, as are many other fast-growth firms operating in other verticals that are now subject to increasing regulatory scrutiny as they reach the scale where their operations start to have a material effect on consumers.

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 2023

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.

Belgium

Dimitri Van Uytvanck, Jérémie Doornaert, Martin Carlier and Mathieu Vancaillie Simmons & Simmons
Marc De Munter Baker Tilly

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. Furthermore, 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 (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.

However, Belgium is generally still lagging behind 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 have a tendency to rely more on organic growth and to focus on underlying services for other companies, with fewer 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 with the Omnibus Law of 27 June 2021 a legal framework for the use of new technologies for the holding and the settlement of securities, in order to allow central securities depositaries (CSDs) and account holders to keep their securities accounts in or through 'secured mechanisms for electronic registration'.

Furthermore, Belgium has not implemented a sandbox. But both the National Bank of Belgium 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 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 (DLT), 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.

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), Self-employed and Energy (FPS Economy) also has 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 stand-alone basis) does not require a licence, but specific rules of conduct apply where 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 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 (UCITS), derivative contracts and instruments. Dealing in foreign exchange spot and forward contracts (on one's own account or as 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. Furthermore, 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. 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 (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 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 ae 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. Furthermore, 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 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 system 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 provide 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 EEA 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, 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 underling the robo-adviser's functioning, the

services it provides will be considered as (semi-)automated investment service 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' (ie, 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.

Furthermore, 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).

Furthermore, 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.

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, Capital Requirements Directive, Solvency II, Markets in Financial Instruments Directive (MiFID II), Insurance Mediation Directive, Insurance Distribution Directive, Mortgage Credit Directive, Undertakings for Collective Investments in Transferable Securities Directive, Alternative Investment Fund Managers Directive, Payment Services Directive or 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.

Furthermore, 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 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 for 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.

Furthermore, 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.

CHANGE OF CONTROL

Notification and consent

20 | 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

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

The Act of 20 July 2020 transposed the 5th AMLD Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018.

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 the 5th AMLD Directive, two types of virtual currency service providers (ie, 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

22 | 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.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

As a general rule, there are no documentary or execution requirements applicable to loan and security agreements (other than security over real estate), which can be signed by private contract and in counterparts (with as many originals as there are parties to the agreement). The nature of the collateral will determine the type of security that can be granted, and the formalities required to make it enforceable in relation to third parties. The revision of the legal regime applicable to security interests in movable assets (which came into force in early 2018), whereby it became possible to perfect such security by way of filing in a central register. Consumer loans, however, are subject to specific formal and content legal requirements.

In the current Belgian market, peer-to-peer loans generally do not involve security agreements as they operate outside the traditional banking network. As long as all the required formalities are fulfilled, however, it should be possible to structure secured loans.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

The formalities for assignment will depend on how the lending is structured (via a loan agreement or a debt instrument and through a direct or an indirect model).

As a general rule, and in the absence of any contractual provisions prohibiting the transfer, the transfer of a loan agreement by the lender requires the express prior consent of the borrower (as an agreement involves both rights and obligations for both parties). Such consent may be granted in the loan agreement itself. Alternatively, the lender can transfer only its rights (ie, its receivable in relation to the borrower) without the express consent of the borrower. Indeed, according to article 1690 of the old Belgian Civil Code, the transfer of a receivable or right is valid between parties (transferor and transferee) and enforceable in relation to all third parties other than the assigned debtor (ie, the borrower) by the mere conclusion of the transfer agreement. However, the transfer will only become enforceable in relation to the borrower once the transfer is notified to it or once the borrower has acknowledged the transfer. In practice, if (and as long as) the assignment is not perfected, this means that repayment is validly made to the initial lender. The latter can act as servicer for the receivables, which, in practice, avoids having to notify the borrowers upfront.

The transfer of consumer loans is subject to specific rules. If security rights are attached to the loans, additional formalities may also be required.

The formalities to transfer a debt instrument depend on the type of instrument (bearer, registered or dematerialised) and whether the latter is freely negotiable or not.

If the applicable transfer formalities are not fulfilled, the transfer could be held to be unenforceable towards the borrower and possibly third parties.

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

Yes, the EU risk retention rules apply to securitisations of loans originated on a peer-to-peer or marketplace lending platform (P2P securitisations). The risk retention requirements set out in the sectoral EU legislation will apply to P2P securitisations that are offered to European banks, investment firms, alternative investment funds or insurers. Under the current sectoral EU risk retention rules, certain investors (such as credit institutions, Markets in Financial Instruments Directive-regulated firms and firms regulated under the Alternative Investment Fund Managers Directive) will be subject to higher regulatory capital charges where they invest in securitisation positions that do not comply with the risk retention rules.

Those rules require that either the sponsor, originator or original lender in respect of the securitisation explicitly discloses to the investor that it will retain, on an ongoing basis, a material net economic interest in the securitisation (which in any event is not less than 5 per cent) using one of five prescribed retention methods. Those methods include, among other things, retention of:

- the most subordinated tranches, so that the retention equals no less than 5 per cent of the nominal value of the securitised exposures;
- 5 per cent of the nominal value of each of the tranches sold to investors; or
- randomly selected exposures equivalent to no less than 5 per cent of the nominal value of the securitised exposures.

The definitions of 'sponsor', 'original lender' and 'originator' as used in the sectoral EU legislation are set out in Regulation (EU) 2017/2402.

Since 1 January 2019, there has been a direct requirement on the sponsor, originator and original lender to agree on an entity that will act as retention holder and to ensure compliance with the retention requirement. In the absence of agreement among the originator, sponsor and original lender as to who will be the retention holder, the originator will be the retention holder. Definitions of 'sponsor', 'originator' and 'original lender' are set out in the EU Securitisation Regulation.

The EU Securitisation Regulation does not explicitly set out the jurisdictional scope of the 'direct' retention obligation, but there is a helpful note in the Explanatory Memorandum to the European Commission's original proposal for the EU Securitisation Regulation that the intention is that the 'direct' approach would not apply to securitisations (including P2P securitisations) where none of the originator, sponsor or original lender is 'established in the EU'. 'Establishment' is typically described by reference to the jurisdiction in which the legal entity is incorporated or has its registered office. Therefore, the non-EU subsidiary of an EU entity may not be subject to the 'direct' retention obligation because a subsidiary is typically a separate legal entity, whereas a non-EU branch of an EU entity may be caught within this provision because a branch is typically not a separate legal entity. Market participants are still seeking clarity on this and it is expected that this point will be raised as part of the ongoing European Banking Authority (EBA) consultation on risk retention.

Possible retaining entities in respect of P2P securitisations

Typically, a peer-to-peer lending platform will not qualify as the 'sponsor', 'originator' or 'original lender' of a P2P securitisation, and another entity with the capacity to retain will, therefore, need to be identified. The range of entities with capacity to retain is broader under the EU Securitisation Regulation than under the current EU sectoral legislation and, therefore, the ability of an entity to retain will depend on the rules that apply at the time the securitised notes are issued.

Any entity that retains in the capacity of 'originator' is expected to be an entity of substance, and the EU Securitisation Regulation expressly provides that an entity shall not be considered to be an originator where it has been established or operates for the sole purpose of securitising exposures. The EU Securitisation Regulation does not specify in what circumstances an entity will be considered to have been established for the sole purpose of securitising exposures but, in December 2017, the EBA published a consultation paper that proposed that an originator will not be considered to have been established with the 'sole purpose' of securitising exposures if it satisfies certain conditions, including that:

- it has a broader business enterprise and strategy;
- it has sufficient decision makers with the required experience; and
- its ability to make payment obligations depends neither on the exposures to be securitised nor on any exposures retained for the purposes of the risk retention regulations.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

The entity assigning loans to the special purpose vehicle (SPV) must ensure that there are no confidentiality requirements in the loan documents that would prevent it from disclosing information about the loans and the relevant borrowers to the SPV and the other securitisation

parties. If there are such restrictions in the underlying loan documentation, the assignor will require the consent of the relevant borrower to disclose to the SPV and other securitisation parties the information they require before agreeing to the asset sale.

In addition, the SPV will want to ensure that there are no restrictions in the loan documents that would prevent it from complying with its disclosure obligations under Belgian and EU law (such as those set out in the Credit Rating Agency Regulation). Again, if such restrictions are included in the underlying loan documents, the SPV would be required to obtain the relevant borrower's consent to such disclosure.

Furthermore, if the borrowers are individuals, the SPV, its agents and the peer-to-peer platform will each be required to comply with the statutory data protection requirements under Belgian law.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 | 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 in Belgium.

Distributed ledger technology

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

Distributed ledger technology is in a developmental phase and, as a consequence, it is not yet subject to specific legal or regulatory rules or guidelines. 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, 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 (NBB) via the 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 the 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 EEA following Schrems II case law) in that respect are 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

29 | 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: (1) 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 in order 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 (2) 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 (ie, entities incorporated under Belgian law or EU entities with a Belgian branch, distributor or other form of lasting (electronic) infrastructure in Belgium – eg, ATM machines) are required to register with the FSMA for 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 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 type of infrastructure).

Token issuance

30 | 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 on 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.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 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.

The GDPR also provides a set of rights for the data subjects, including the right to information, the right to access to 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.

Cybersecurity

32 What cybersecurity regulations or standards apply to fintech businesses?

Belgium has implemented Directive (EU) 2016/1148 (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 for 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.

The Payment Services Directive (EU) 2015/2366 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.

Furthermore, Regulation (EU) 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 EU.

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) 526/2013, and on 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 for 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 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

33 | 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

34 | 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.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

35 | 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 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 Belgian Code of Economic Law) and, in certain circumstances, by sui generis database right (Book XI, Title 7 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 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

36 | 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 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 above-mentioned computer programs), IP that is created by an employee in 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 (ie, 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 IP

developed by a contractor or consultant. Therefore, contracts must be carefully drafted.

Joint ownership

37 | 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

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

Belgium mainly implemented the Trade Secrets Directive (EU) 2016/943 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 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

39 | 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

40 | 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 custom authorities for border detention.

COMPETITION

Sector-specific issues

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

Competition law (ie, 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 into 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 procompetitive effects of fintech needs 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 (ie, 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

42 | 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 if the start-up is 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 2022) and this 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 employer is 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 environmental friendly R&D investments and patents of 13.5 per cent of the acquisition value, which can be increased to 25 per cent for investments in 2021 and 2022 if the investor is a 'small' (SME) company; and
- private individuals trading in bitcoins are not necessarily taxed on the gains as professional income, but insofar 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

43 | 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 OECD work on the digitalised economy. In particular, the current focus is on the OECD/G20 Inclusive Framework (Pillar One on revised nexus and

simmons+simmons

Dimitri Van Uytvanck
dimitri.vanuytvanck@simmons-simmons.com

Jérémie Doornaert
jeremie.doornaert@simmons-simmons.com

Martin Carlier
martin.carlier@simmons-simmons.com

Mathieu Vancaillie
mathieu.vancaillie@simmons-simmons.com

Avenue Louise 143
1050 Brussels
Belgium
Tel: +32 2 542 09 60
Fax: +32 2 542 09 61
www.simmons-simmons.com

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

profit allocation rules and Pillar Two on 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 a tax reform, shifting taxation from labour to other types of income and profits.

IMMIGRATION

Sector-specific schemes

44 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 a longer period than 90 days, foreign workers must have a valid work permit. This condition does not apply to nationals of a member state of the EEA (the countries of the EU 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.

There are no special regimes specific to the fintech sector.

UPDATE AND TRENDS

Current developments

45 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 crypto-currencies and will definitely play an important role in the near future.

Canada

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

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, have continued to experience significant growth. The pace of innovation has 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 are leading the charge in many cases, fintech start-ups are a key part of the fintech ecosystem across the nation. In the cryptocurrency sector, Canadian regulators have shown leadership in providing a 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. Future prospects include major investments in AI-driven fintech solutions, blockchain, reg-tech and, in the insurance industry where Canada is a significant global player, in insurtech.

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, as detailed below, are actively encouraging 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 anticipated Retail Payments Activities Act (RPAA) (Bill C-30, An Act Respecting Retail Payment Activities, 2nd Sess, 43rd Parl, 2021, cl 177 (assented to 29 June 2021);
- federal regulatory and support initiative for open-banking/consumer-driven finance;
- notices and an actionable roadmap by the Canadian Securities Administrators guiding the services and uses related to crypto currency 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), working 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). 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 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/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 (ICOs) 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' (ie, an entity that brings together multiple buyers and multiple sellers of securities or derivatives), the CSA has further noted that fintech businesses involved in cryptocurrencies should 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 reporting, record keeping, KYC 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 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 relative to certain other jurisdictions. Nevertheless, aspects of consumer lending are regulated in Canada at both the federal and provincial level. At the federal level, the regulation depends on the regulated status of the entity providing the 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 (ie, 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 are 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 requirements. 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.

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 are subject to provincial prospectus requirements or, in the case of private placements, related exemption requirements, as well as 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 NI 81-104 primarily focused on AIFs and allowing for adoption of fundamental investment objectives that permit AIFs to engage in certain investment strategies (eg, short-selling, borrowing, use of derivatives) that are not 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 will come into force 21 September 2021.

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. Further, 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, was originally set to replace the current Large Value Transfer System by 2021. Lynx will enable payment and settlement finality and flexibility for the application of future technologies, as well as enhanced cyber security capabilities. The RTR is set to launch in 2022 and 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 RPAA will apply to all retail payment activities performed by payment service providers (PSP) 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, PSPs 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 the Consumer Privacy Protection Act (Bill C-11, Consumer Privacy Protection Act, 2nd Sess, 43rd Parl, 2020, cl 2 (first reading 17 November 2020)), 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.

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 conducting KYC obligations, participating in due diligence reviews and participating in compliance reviews by CSA staff. The CSA has generally declined to grant exemptive relief for robo-advisers from NI 31-103 and related rules.

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. 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 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.

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 foreign money services business (MSB) 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.

CHANGE OF CONTROL

Notification and consent

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

MSBs 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 (IIROC) pursuant to IIROC's 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 anti-trust and competition regulations may also impose notification or approval requirements.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

21 | 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, KYC and other 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 FINTRAC's AML and ATF compliance requirements, including

compliance programme, KYC, reporting, recordkeeping and other requirements. Additional requirements apply under the Criminal Code, the Corruption of Foreign Public Officials Act (SC 1998, c 34) and Canadian sanctions legislation.

Guidance

22 | 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 MSBs 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.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

In Canada, there is a risk that certain loan or security agreements will not be enforceable where borrowers default on their loans. Lenders generally rely on peer-to-peer (P2P) lending companies' credit analytics and default management services to gauge the creditworthiness of a borrower. This subjects the lender to both credit risk from the borrower and risk from the integrity of the platform, typically without forms of insurance that may be provided by certain banks.

If the borrowers are consumers, there are numerous requirements under provincial consumer protection legislation pertaining to 'credit agreements', 'internet agreements' and 'remote agreements', among others, which if not complied with could render an agreement unenforceable or subject to cancellation by the consumer. In very general terms, the consumer protection legislation for credit agreements imposes (often quite specific) cost-of-borrowing disclosure obligations and prohibits a wide range of unfair practices. Actual execution of a loan contract by electronic signature is generally permitted, even for consumers, subject to the requirements described above. Loans offered in compliance with provincial securities laws are exempt from the consumer protection requirements, on the basis that retail investors are adequately protected under the securities legislation.

Assignment of loans

24 | What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

Canadian securities regulators have taken a cautious approach to loans originated on P2P marketplace lending platforms and have determined that such loan arrangements may constitute "securities". Generally, a borrower must grant a security interest to a lender in investment property to secure its payment obligations and that interest must attach. A secured lender can then perfect its interest by (1) registering a financing statement in accordance with the Personal Property Security Act, (2) taking possession or (3) obtaining effective control of the collateral. However, P2P lending involves a higher degree of risk. In many cases, lenders may rely on default management services provided by P2P lending companies.

It is possible for investors to purchase loans from P2P lending platforms and act as third-party debt collectors without informing the borrower when no changes are made to the terms of the loan.

Securitisation risk retention requirements

25 | Are securitisation transactions subject to risk retention requirements?

There is no requirement for risk retention on the part of a sponsor or seller in a Canadian securitisation. However, if securities issued in a Canadian transaction are offered to US or EU investors, US or EU risk-retention rules may apply to the transaction.

Securitisation confidentiality and data protection requirements

26 | Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

The nature of the assets securitised, the location of the participants to a securitisation and the process used to purchase these loans will determine the legislation and regulations applicable. However, most applicable federal and provincial regulations outline some level of confidentiality required regarding user data. For example, federal and provincial consumer protection and privacy legislation, as well as regulations applicable to financial institutions, impose a certain level of confidentiality relating to borrower information.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

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

The regulation of 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 Customer 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.

Furthermore, 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.

Distributed ledger technology

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

The Canadian federal government is currently 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. 'Stablecoins', crypto assets backed fully or in part by currency of commodity holdings, are considered by the BoC to 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.

Cryptoassets

29 | 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 CSA and the Investment Industry Regulatory Organization of Canada (IIROC) 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 reporting client identification, recordkeeping, reporting and other AML programme compliance requirements.

Token issuance

30 | 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 MSBs (or in the case of non-Canadian exchanges or platforms, foreign MSBS or FMSBs). These entities must follow specific obligations imposed by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act 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.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 | 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. The Act applies 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 (ie, 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.

Cybersecurity

32 | 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 certification and standards that are appropriate for the organisation's industry.

Canadian regulators and self-regulatory organisations (including the CSA, IIROC, OSFI 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. Fintech businesses that are 'reporting issuers' (ie, 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 (ie, 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.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

33 | 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 Guidelines). The B-10 Guidelines address 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 guidelines include 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 Guidelines do not technically have the force of law, they are 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 addition, OSFI requires that federally regulated financial services companies conduct cyber risk self-assessments and OSFI will assess cyber risk as part of its overall prudential supervisory review. OSFI has also stated that it views 'operational resilience' (to which cyber-risk is relevant) as an important objective of operational risk management and, as a result, critical for the overall safety and soundness of a financial institution.

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 discloses personal information under its custody or control to a third party (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.

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

34 | 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

35 | 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 up 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

36 | 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 owner 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

37 | 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-owner's 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-owner's consent unless doing so would dilute the co-owners' rights.

Trade secrets

38 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 which 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

39 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 IP with registrations and documentation to control ownership and use of its IP rights, including permitted use under licensing and collaborative agreements with third parties.

In order 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

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

IP rights holders, not CIPO, are responsible for enforcing their IP rights. Remedies for infringement include seeking damages sustained as results 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

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

There are 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 entitled '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.

TAX

Incentives

42 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$3,000,000 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

43 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 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.

The federal government announced its plan to introduce a Digital Services Tax (DST) in its 2021 Federal Budget. The DST is set to take effect in January 2022 until an acceptable multilateral approach takes effect. While the draft legislation has not been released yet, the Budget revealed some of its key features: the DST would apply at the rate of 3 per cent on revenue generated from online business models such as online marketplaces, social media platforms, online advertising and user data. Contrary to the excise tax provision, it will apply to domestic and foreign companies, but only to those who have €750 million or more in global revenue from all sources in the preceding year, and in-scope revenue associated with Canadian users over C$20 million in that year. The draft legislation was set for the summer of 2021.

IMMIGRATION

Sector-specific schemes

44 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 white 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 Talen Stream programme (the Program), was implemented by the federal government to help Canadian businesses recruit individual 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

45 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 global 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 AI technologies.

* *The information in this chapter was accurate as at August 2021.*

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 St
Toronto
ON M5L 1B9
Canada
Tel: +1 416 869 5500
www.stikeman.com

China

Jingyuan Shi, Yuchen Lai and Yanyu Lai

Simmons & Simmons

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, 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 blockchain-based currency, online insurance, the centralised storage of deposits in payments sectors, 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, artificial intelligence, green and low carbon emission, fair and inclusiveness; the Fintech Plan also sets the development goals, including digital transformation in financial industry, full use of data resources, improved financial service quality and efficiency, mature governance system for fintech industry, use of core tech applications, 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 next four years. 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 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 end of April 2022, over 150 fintech applications had been covered by the sandbox schemes.

The relevant provinces and cities have 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.

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 Banking and Insurance Regulatory Commission (CBIRC) and China Securities Regulatory Commission (CSRC).

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;
- 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;
- carrying on fund management services;
- carrying on fund custodian services;
- carrying on derivative products transactions;
- lending micro loans online or offline;
- providing consumer finance services;
- providing third-party payment services;
- providing financial lease services;
- carrying on futures trading services;
- providing credit services;

- providing commercial factoring services; and
- operating financial holding companies.

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 CBIRC also issued the Trial Rules for Supervision Rating for Consumer Finance Companies.

According to the General Rules of Loans, to engage in 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 must be approved by the CBIRC.

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

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 CBIRC and the following restrictions:

- the financial institutions must report certain information to 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 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. Currently 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 of 1.14 billion yuan was successfully transferred in September 2021.

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 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 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 fund raising, 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 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 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 order, promissory note and cheque. 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 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 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 of prepaid cards;
- acceptance of payments using a bank card; 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, payment services providers will need to obtain a licence from the foreign exchange authority (ie, the State Administration of Foreign Exchange (SAFE)), in addition to the payment licence issued by the PBOC. 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.

The PBOC published a draft Regulation on Non-banking Payment Agencies in January 2021. This draft regulation re-classifies payment services into two types: operation of prepaid accounts and processing of payment transactions. It provides rules regarding the incorporation, licensing, operation and supervision of non-banking payment agencies within China. The draft regulation also brings in provisions regarding personal information protection and anti-monopoly supervision. As of June 2022, the draft regulation is still pending finalisation.

According to the legislation plan issued by the PBOC on 17 April 2020, the drafting of the 'Measures for the Administration of Cross-border Payment Services' has been put on the agenda to further regulate cross-border payment services. However, as of June 2022, there is no subsequent development on these draft measures.

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 mechanism 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 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 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.

In addition, some cities, such as Shanghai and Beijing, have issued incentive plans for new businesses that include robo-advisers.

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 CBIRC. Insurance companies and brokers must be CBIRC-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 (these third-party online platforms are not required to be CBIRC-licensed because all the insurance-related activities are, and must be, conducted by the licensed insurance companies and brokers, instead of the platform operator).

In October 2021, the 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 business online.

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 are the primary regulations for credit references and credit information services. The providers of 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.

In 2018, the PBOC issued its first personal credit rating business licence to Baihang Credit Co, Ltd, a newly established company comprising the eight companies and the National Internet Finance Association as its shareholders. In December 2020, the PBOC issued its second personal credit rating business licence to Pudao Credit Co, Ltd, a joint venture with shareholders from a major Beijing local government controlled financial group and leading private companies. In November 2021, the PBOC announced that it had accepted the application from Qiantang Credit Co, Ltd for the third personal credit rating licence. Public record shows the largest shareholder of Qiantang Credit is Ant Group, accounting for 35 per cent of its equity.

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 (PBOC), China Securities Regulatory Commission (CSRC) and China Banking and Insurance Regulatory Commission (CBIRC), 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 (CSRC) and the sale of insurance products is subject to the approval of the China Banking and Insurance Regulatory Commission (CBIRC).

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 loss 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.

CHANGE OF CONTROL

Notification and consent

20 | 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

21 | 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 China Banking and Insurance Regulatory Commission (CBIRC), 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 review 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 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

22 | 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. Scope and boundary of prosecution and explanation of the definitions of several high-profile crimes were discussed.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

There are no specific legal requirements for executing loan agreements or security agreements in China.

The Interim Measures for the Administration of Business Activities on Online Lending Information Intermediary Agencies, issued by the China Banking and Insurance Regulatory Commission (CBIRC) on 17 August 2016, provide that online lending platforms are designated as information intermediaries for borrowers and lenders and must not provide credit enhancement or security or guarantee arrangements for the loan transactions by itself.

Therefore, a peer-to-peer lending platform is merely an information exchange. Even if loan and security agreements are entered into on the peer-to-peer marketplace, it does not impact the legal effectiveness and enforcement of loan agreements or security agreements, provided that such agreements are duly executed in accordance with the relevant laws.

Assignment of loans

24 | What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

According to the Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Private Lending Cases and the Civil Code, the legal assignment of a loan by the assignor (ie, the lender) to the assignee (ie, the purchaser) will be perfected provided that:

- the following circumstances are not applicable to the assignment: the rights may not be assigned in light of the nature of the contract, according to the agreement between the parties and according to the provisions of the laws;
- a notice of the assignment has been given to the borrower;
- the assignor absolutely assigns the receivable to the assignee; and
- where the laws or administrative regulations stipulate that the assignment of rights or transfer of obligations shall undergo approval or registration procedures, these provisions shall be followed.

If the assignment is not perfected, it may still constitute an equitable assignment (in contrast to a legal assignment), which is still recognised by Chinese courts. However, the disadvantage of an undisclosed assignment is that, in the event of taking any legal action against the borrower for payment, the assignee would have to join the assignor in any such legal action against the borrower (in contrast to being able to sue in its own name in the case of legal assignment) and the assignee may be vulnerable to, among other things, certain competing claims and other set-off rights that may otherwise have been halted by the serving of notice on the borrower.

It is not possible to transfer loans to the purchaser without informing the borrower. Unless the borrower is notified, the assignment shall not be binding on the borrower. This notice by the assignor to assign its rights must not be revoked, unless such revocation is consented to by the assignee.

Securitisation risk retention requirements

25 | Are securitisation transactions subject to risk retention requirements?

Yes. The PBOC and the China Banking Regulatory Commission (CBRC, predecessor of the CBIRC) issued a notice in December 2013 to regulate the risk retention of asset securitisation originators. The originators are required to retain risk by holding at least 5 per cent of the securitised assets.

Securitisation confidentiality and data protection requirements

26 | Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

The peer-to-peer platform operator must keep the lender's and borrower's information confidential, and further processing activities of data from the subjects in China must be carried out in China. The purchaser is subject to data protection requirements under the Data Security Law (effective from 1 September 2021) and the Personal Information Protection Law (effective from 1 November 2021).

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 | 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 (PBOC), China Banking and Insurance Regulatory Commission, China Securities Regulatory Commission and 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 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 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 (CAC), 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.

Distributed ledger technology

28 | 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 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 the operating permits under those rules. Although there is no operating permits requirement on 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 PBOC published an industry standard regarding Financial Distributed Ledger Technology Security Specification.

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 mechanism 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.

Cryptoassets

29 | 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 crypto business, including but not limited to:

- Bitcoin, ETH and USDT 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 is 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 Cyberspace Administration of China (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 is prohibited in China.

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. So far, the tests have been launched in dozens of major Chinese cities. But it is still unclear when PBOC will officially issue digital currency.

However, the DCEP is fiat money, and its development does not in any way suggest a change in the regulator's attitude towards cryptocurrencies.

Token issuance

30 | 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.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 | 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 Cybersecurity Law provides the general principles of use and processing of personal data in China including, among others:

- the collection, use and processing of personal data shall be legitimate, reasonable and necessary;
- data subjects shall be informed of the purpose, scope, method and rules of data collection and processing, rights to access and correct personal data, and the implications for refusal of data collection or processing; and
- the consent of data subjects shall be obtained prior to any collection, use, processing or transfer of his or her personal data.

In addition, the Cybersecurity Law requires that personal information and important data collected or gathered by the Critical Information Infrastructure (CII) operators during their operations is stored within the territory of China. Where it is necessary to provide this information and data to overseas entities owing to business demands, a security assessment must be conducted.

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. Cross-border transfer of such important data will be subject to security assessment organised by the Cyberspace Administration of China (CAC) (for CII operators) or other rules set out by the CAC (for other organisations).

The PIPL became effective on 1 November 2021. The law has extra-territorial 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.

In addition, the PIPL provides more legal bases for data processing besides consent. It also sets out several legal requirements for the cross-border transfer of personal data, including:

- obtaining a separate informed consent from the data subjects;
- conducting a prior data protection impact assessment; and
- completing a security assessment organised by the CAC (for CII operators and processors of a large quantity of personal data exceeding the volume threshold determined by the CAC), or following a voluntary security assessment, a certification of personal data protection by designated agencies or conclusion of a standard transfer agreement with the foreign recipient (for other organisations).

In addition to the above three key regulations, 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 the consumer financial information. Financial institutions are required to notify the relevant local branches of the 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 information 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 transfer.

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 be transferred via safe channels or in the form of encrypted data.

Cybersecurity

32 | 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.

Several industrial standards published by the PBOC cover specific cybersecurity issues of financial institutions, such as disaster recovery, data centre management, infrastructure of non-banking payment agencies, cloud computing applications, etc. Three standards published in October 2020 are in particular close 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

33 | 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 China Banking and Insurance Regulatory Commission (CBIRC) 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 sub-contract any outsourcing business to third parties.

On 30 December 2021, the 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.

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

34 | 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 centre, 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 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

35 | 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 works. 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 of 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

36 | 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 works 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. Furthermore, 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

37 | 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

38 | 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 on. 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

39 | 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 State Intellectual Property Office of China, 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

40 | 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

41 | 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 wrong doings, taking into account the nature and characteristics of platform economy. The State Administration of Market Regulation has initiated several high-profile cases against platform giants. Large fintech platforms are potential enforcement targets, too.

TAX

Incentives

42 | 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 VAT exemption and income tax reduction until the end of 2023.

Increased tax burden

43 | 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

44 | 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 to work in China. Eligible applicants can be issued visas that are valid for five to 10 years with multiple entry.

UPDATE AND TRENDS

Current developments

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

Following the promulgation of Data Security Law and Personal Information Protection Law (PIPL) in the second half of 2021, various Chinese regulators, including but not limited to the 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.

Jingyuan Shi
jingyuan.shi@simmons-simmons.com

Yuchen Lai
yuchen.lai@simmons-simmons.com

Yanyu Lai
yanyu.lai@simmons-simmons.com

25th Floor Kerry Centre South Tower
1 Guang Hua Road
Chaoyang District
Beijing
100020
China
Tel: +86 10 8588 4500
Fax: +86 10 8588 4588
www.simmons-simmons.com

Denmark

Rasmus Mandøe Jensen and Jónas Már Torfason

Plesner Advokatpartnerselskab

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 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 Financial Supervisory Authority, enabling it to dedicate resources to a specialised fintech office and create a regulatory sandbox. The Financial Supervisory Authority opened applications for its regulatory sandbox in 2018 and has published notes on projects examined in the regulatory sandbox as recently as February 2022, where a blockchain-based payment solution was examined. According to the Financial Supervisory Authority, this was the first time that a supervisory authority within the EU had carried out an assessment based on a specific business model.

In terms of purpose and eligibility criteria, the sandbox is similar to the existing one operated by the UK Financial Conduct Authority.

FINANCIAL REGULATION

Regulatory bodies

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

The main financial regulator is the Financial Supervisory Authority, which also oversees compliance with anti-money laundering regulation.

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 Financial Supervisory Authority'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 the revised EU Payment Services Directive (2015/2366/EU) (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 the PSD2 and article 1 of the Second EU Electronic Money Directive (2009/110/EU) (EMD2), except that technical services covered by the exemption in article 3(j) of the PSD2 are subject to certain fee regulations in the Payments Act.

Specifically, regarding the limited network exemption (article 3(k) of the PSD2 and article 1(4) of the 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 the PSD2 and article 11 of the 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 the PSD2 and article 9 of the 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 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 the EU Markets in Financial Instruments II Directive (MiFID) – 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 and the Investment Firms Directive (2019/2034/EU).

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 the EU Alternative Investment Fund Managers Directive, whereas a registered manager must comply with only a few limited requirements.

The definition of 'alternative investment funds' has been implemented from the EU Alternative Investment Fund Managers Directive 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 Financial Supervisory Authority 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 Financial Supervisory Authority (as 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 undertaking is carried out on television or on-demand services or in connection with gambling or betting, or both, the marketing prohibition will apply.

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.

Depending on the nature of the activity, fintech businesses may be subject to one or more of the following laws, each of which include associated delegated regulations:

- the Payments Act (implementing the PSD2 or the EMD2), if the activity involves offering payment services or issuing e-money;
- the Investment Association Act (implementing the EU Undertakings for Collective Investment in Transferable Securities Directive (2009/65/EU)), if the activity involves establishing or managing undertakings for collective investment in transferable securities;
- the Act on Alternative Investment Fund Managers (implementing the EU Alternative Investment Fund Managers Directive (2011/61/EU) (AIFMD)), if the activity involves establishing or managing an alternative investment fund;
- the Capital Markets Act and the EU Market Abuse Regulation (2014/596), 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
- the European Crowdfunding Service Providers Regulation (2020/1503) if the activity involves the matching of business funding interests of investors and project owners through the use of a crowdfunding platform and which consists of either (1) the facilitation of granting of loans or (2) 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 (2014/596) 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 (2020/1503) applies if the activity involves the matching of business funding interests of investors and project owners through the use of a crowdfunding platform and which consists of either (1) the facilitation of granting of loans or (2) 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 Financial Supervisory Authority, 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 the 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 the 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 Financial Supervisory Authority 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/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 the EU Alternative Investment Fund Managers Directive (2011/61/EU)).
- The Markets in Financial Instruments Directive (2014/65/EU).
- The Consumer Contracts Act (implementing parts of the EU Directive on Consumer Rights (2011/83/EU) and the EU Directive on Distance Marketing of Consumer Financial Services (2002/65/EU)), which contains rules on pre-contractual information requirements, right of withdrawal, termination and binding periods.
- The Marketing Practices Act (implementing the EU Directive on Unfair Commercial Practices (2005/29/EU)), 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.

- The Payments Act (implementing the Payment Services Directive (2015/2366/EU)), 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 the Second EU Electronic Money Directive (2009/110/EU)).
- The Credit Contracts Act (implementing parts of the EU Consumer Credit Directive (2008/48/EU)), 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 the EU Directive on Consumer Rights), 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 the EU Insurance Distribution Directive (2016/97/EU)), if the activity involves insurance distribution.

CHANGE OF CONTROL

Notification and consent

20 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 Financial Supervisory Authority. 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 Financial Supervisory Authority pursuant to the Anti-money Laundering Act, there would be a de facto consent requirement from the Financial Supervisory Authority in the event of a change of control, as the Financial Supervisory Authority 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

21 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

22 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) have prepared and published guidelines to the Act on Measures to Prevent Money Laundering and the Financing of Terrorism, which can be found on the website of the Danish FSA.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

There are no specific requirements for executing loan agreements or security agreements other than authorisation and execution of a loan or security agreement. As peer-to-peer lending marketplace lending platforms are not subject to bespoke regulation, there is no specific risk that the agreements in question would not be enforceable.

However, the Act on Consumer Loan Undertakings includes a 35 per cent cap on the annual percentage rate (APR) on consumer loans, including on peer-to-peer loans to consumers. To the extent that a consumer loan agreement has APR higher than the 35 per cent cap and the lender does not hold a licence as a consumer loan provider or is licensed as a financial institution, the lender will only be entitled to demand repayment of the principal (ie, repayment without any interest). To the extent that the lender holds a licence as a consumer loan provider or is licensed as a financial institution, the lender would in this case only be entitled to demand repayment of the principal together with costs (the interest and fees, etc) up to an APR of 35 per cent.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

In the relationship between an assignor and assignee, the transfer of the assignment will be effective once an assignment agreement has been entered into. However, for the sale to be effective against any creditors of the assignor and the bankruptcy estate of the assignor, the assignee (or the assignor, or both) must notify the relevant borrower of the sale and inform it to redirect payments under the loan to the assignee.

If an assignment has not been duly perfected, it may be voided subject to a hardening period, pursuant to which it may become voidable and unenforceable. In the case of unaffiliated parties, the normal hardening period under Danish law is three months.

Therefore, it is impossible to complete the perfection requirements without informing the borrower. However, in the relationship between the assignor and assignee, the borrower need not be notified to validate the assignment.

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

There are no specific Danish law risk retention requirements; however, the rules on risk retention requirements set out in the Capital Requirements Regulation may apply.

Securitisation confidentiality and data protection requirements

26 | Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

Such special purpose vehicles are subject to both the EU General Data Protection Regulation and the Danish Data Protection Act.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

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

AI is not subject to bespoke regulation in Denmark. In July 2019, the Financial Supervisory Authority published a regulatory note regarding best practice when using supervised machine learning. Furthermore, on 21 April 2021, the European Commission published a proposal for a directive to regulate artificial intelligence that aims to promote the development of artificial intelligence and address the risks it poses to safety and fundamental rights.

Distributed ledger technology

28 | 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. On 24 September 2020, the European Commission published a proposal for (1) a new draft regulation comprised of a draft six-year pilot regime on distributed ledger market infrastructure, which sets out the requirement on multilateral trading facilities and securities settlement systems using DLT (currently adopted and awaiting publication in the Official Journal)) and (2) a draft directive for a proposal to amend the existing definition of 'financial instruments' pursuant to MiFID II (2014/65/EU) to include such instruments issued by means of DLT.

Cryptoassets

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

Cryptoassets and digital currencies are not subject to bespoke regulation. Digital wallets and e-money are subject to the EU rules pursuant to the revised EU Payment Services Directive (2015/2366/EU).

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; and
- issuers of cryptocurrencies.

In addition, on 24 September 2020, the European Commission published a draft regulation of markets in cryptoassets (MiCA), which includes regulation specifically aimed at utility-tokens, stablecoins and e-money tokens. The MiCA regulation was adopted by the European Parliament on 14 March 2022 and is entering into the next steps of the legislative process.

Token issuance

30 | 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 Financial Supervisory Authority. Furthermore, the draft MiCA regulation contains a proposal for regulation of 'crypto-asset service providers', which includes digital currency exchanges and brokerages.

DATA PROTECTION AND CYBERSECURITY

Data protection

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

The EU 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, CPR 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. Furthermore, if data is transferred outside the European Union, a legal basis for the transfer must be in place.

Cybersecurity

32 | 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 Secure Open Standards of Communication (Commission Delegated Regulation (EU) 2018/389);
- the Guidelines on the Security Measures for Operational and Security Risks of Payment Services (promulgated under the revised EU 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

33 | 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 Financial Supervisory Authority 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 goes beyond the outsourcing guidelines of the European Banking Authority.

The Outsourcing Order sets out specific requirement for the outsourcing of 'critical or important' areas, including detailed requirements for the outsourcing agreement between the company and the outsourcing provider; for example, 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 Financial Supervisory Authority has published official guidelines to the Outsourcing Order.

Cloud computing

34 | 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 Financial Supervisory Authority 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

35 | 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 the EU Directive on the Legal Protection of Databases (96/9/EU)) 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 the EU Directive on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) (2016/943/EU)) if the innovation is kept secret.

IP developed by employees and contractors

36 | 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.

Further, 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 transfer 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.

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

37 | 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 in 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

38 | 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 EU Directive on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) (2016/943/EU)) 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

39 | 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 reproduce the trademark in an appropriate manner by using technology that is generally available in order 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

40 | 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

41 | 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 anticompetitive behaviour may arise in certain circumstances.

TAX

Incentives

42 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 a couple of specific incentive rules concerning R&D.

Firstly, 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 kroner annually.

In addition, there is another regime – the 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 kroner annually (ie, a maximum annual payout of 5.5 million 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.

Increased tax burden

43 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 under way.

IMMIGRATION

Sector-specific schemes

44 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 EU, EEA 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 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 (448,000 kroner in 2022) and the employment terms correspond to Danish standards;
- the Positive List scheme, under which residence and work permits are granted to employees who have been offered jobs that are listed on the Positive List 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.

PLESNER

Rasmus Mandøe Jensen
rmj@plesner.com

Jónas Már Torfason
jomt@plesner.com

Amerika Plads 37
DK-2100 Copenhagen
Denmark
Tel: +45 33 12 11 33
www.plesner.com

Additional immigration schemes are available that may be relevant (eg, for trainees or intra-group secondments).

UPDATE AND TRENDS

Current developments

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

There has been significant public discussion on so-called 'Buy Now-Pay Later' (BNPL) schemes. As zero-fee, zero-interest consumer loans are not currently legislated, following negative coverage the Minister of Commerce has signalled that BNPL schemes will be legislated in line with other consumer loans, presumably including a registration requirement, a duty to provide information to potential borrowers and a cool-down period.

Egypt

Mohamed Hashish and Farida Rezk

Soliman, Hashish & Partners

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 201q a4;
- 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;
- 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, cryptocurrency and e-payments. The current government of Egypt has continued and continues to promote financial inclusion and the digitisation of the financial sector within Egypt. In July 2020, the Financial Regulatory Authority (FRA) proposed a draft fintech law to regulate the use of fintech to deliver non-banking financial services (NBFS) in Egypt. This draft was reviewed by the Egyptian House of Representatives, which introduced a number of changes to the said draft, and then the amended draft was approved and issued as the first ever Fintech Law in Egypt. The Fintech Law was published in the Official Gazette on 8 February 2022. The aim of the Fintech Law is to facilitate the integration of technologies into financial services, and regulatory framework for fintech businesses to support NBFS services. It covers services such as robo-advisory, microfinance, insurtech, artificial intelligence, mobile applications and digital platforms

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 CBE launched a regulatory sandbox for the purpose of providing fintech players with is 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 funds initiatives are available to fintech start-ups in Egypt. For example, in March 2019, the Central Bank of Egypt (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 be used also by small and medium-sized fintech players.

In response to covid-19, CBE organised the distribution of free point of sale (POS) terminals, eased fees and charges, and increased contactless payments 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 Central Bank of Egypt (CBE), which is empowered by Law No. 88 of 2003 on the Central Bank of Egypt and the Banking Sector (the Banking Law) 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 (NBFS) 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 of these works within the limits of their establishment.

'Banking activities' are defined under the Banking Law 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 capitals 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 those provisions is subject to imprisonment or a fine 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 those penalties in respect of 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.

Other than the general rule above, 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 aiming 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 consumer finance-related activities above 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 the carrying out of 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 can be carried out unless a licence is obtained from the FRA. Banks registered with the CBE may carry out the activity, provided that an 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 any equivalent currency.

Licensed investment funds must deposit any securities that they are investing in with one of the banks that is registered with the CBE, providing that the bank (and its related parties) does not control or hold more than 10 per cent of the total shares in 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 before establishing them except for in the case of private equity funds and providing, among other things, that a notification is sent to the FRA and that no underwriting is made as a 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?

Yes, 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 meaning of banking activities; however, it may also be a form of 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 around 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 banking activities (if providing credit), and may also be characterised as a factoring. 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 main three 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 a 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 being 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 license 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 exceptions 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 (IPN) 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 introduced regulations on robo-advisers, which are subject to licensing from 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 this restriction and are regulated in Egypt.

Furthermore, the new Fintech Law also regulates insurtech, which is subject to licensing from 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. Those services require a licence from the CBE.

At present, there is only one licensed company, 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 an approval from the person is obtained.

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?

No.

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 a prior licence and approval.

CHANGE OF CONTROL

Notification and consent

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

It depends 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

21 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

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

Yes, all available guides can be found on the anti-money laundering page of the Central Bank of Egypt's website.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

In general, loan agreements do not require any execution formalities, whereas almost all types of securities, such as mortgages, liens, pledges, assignments of rights and movable collateral, have specific execution formalities to be enforceable and effective in respect of third parties.

Peer-to-peer and marketplace lending platforms may be deemed as banking activities; therefore, there is an invalidity risk associated with any loan granted within the peer-to-peer and marketplace lending platform without compliance with the relevant licensing framework.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

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 the carrying out of banking activities, in which case licensing by and registration with the Central Bank of Egypt 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).

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

In general, the originator of a securitisation portfolio must guarantee its existence at the assignment date, and the originator is not liable for settling any dues that are the subject of the portfolio upon the perfection of the assignment to the relevant securitisation special purpose vehicle.

The assignment is required, in general, not to be conditional except for one condition that requires complete subscription to the securitised portfolio.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

Not applicable.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 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, according to Prime Ministerial Decree No. 2889 of 2019, a new national council was established: 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 High Education has started to add special artificial intelligence departments to several engineering universities in Egypt.

The government has created an enabling legal environment to govern the uses of artificial intelligence. This involved the issuing of the Data Protection Law, in July 2020, which regulates the relationship between data owner and users.

Furthermore, robo-advice is now newly regulated under the new Fintech Law, and is subject to licensing from the Financial Regulatory Authority (FRA).

Distributed ledger technology

28 | 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 blockchain. However, the Banking Law prohibits the issuance or trade of cryptocurrencies or electronic money or 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

29 | 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 or 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

30 | 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.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 | 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 applies to any personal data that is subject to electronic processing, whether partially or entirely.

The 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 (the 'centre'), and where the level of protection is less than what is provided for by the Law. The policies and regulations for cross-border transfer shall be specified in the Executive Regulations, which have not been issued yet. After the date of its issuance, any entity subject to the Data Protection Law is required to legitimise its position within one year.

Cybersecurity

32 | 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

33 | 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. 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. These conditions and requirements 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 requires all banks registered with the CBE to meet specific legal requirements, including the provision of a penetration test report to the CBE.

Furthermore, according to 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 in order to perform certain functions and services on their behalf. Accordingly, these delegated service providers must register with the CBE.

Cloud computing

34 | 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 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. Those providers must retain and store users' data for at least 180 continuous 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

35 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

36 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 IPRs 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

37 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 IPRs 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 use any right over the work unless otherwise agreed between the authors in writing.

Trade secrets

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

Trade secrets (including confidential information) are protected by the IPRs 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 IPRs Law, the court will maintain the confidentially of trade secrets.

Branding

39 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 trademarks.

Remedies for infringement of IP

40 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 that cover all the losses incurred to 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

41 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 (the Antitrust Law) and its executive regulations.

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 in the 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 its customers that results in limiting competition.

The assessment of any violation under the Antitrust Law is made by 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

42 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, counting from the date of starting the investment projects in Egypt, subject to a specific formula.

Increased tax burden

43 | 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 tax authority in real time before being sent to the customer. The decree obliges all VAT-registered businesses to issue an electronic invoice containing the issuer's electronic signature and a unified code for the goods or service.

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 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.

Furthermore, according to the Ministry of Finance, VAT is no longer deductible from paper invoices as of January 2022.

IMMIGRATION

Sector-specific schemes

44 | 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

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

Yes, the issuance of the new Fintech Law as 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 announced its intention to start rolling out digital banking licences in accordance with 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 (ABC).

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: +201 00047 0077
www.shandpartners.com

France

Hubert de Vauplane and Judith Smadja
Kramer Levin Naftalis & Frankel LLP

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

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

Fintech is a growing industry in France; according to various studies, there are around 800 active fintech companies developing innovative financial business models. Among those factors, the support of regulatory agencies and public authorities for the fintech industry play an undeniable role, along with the quality of French engineers, the number of incubators throughout the country but also the organisation of numerous forums (eg, the Paris Blockchain Week Summit in April 2022 or the ACPR-AMF Fintech Forum in October 2021). The second half of 2022 will also be busy for the fintech ecosystem. Indeed, France FinTech, Swave, the Prudential Supervision and Resolution Authority (ACPR) and Financial Markets Authority (AMF) announced in April 2022 the second edition of the French FinTech Week, dedicated to the actors of the innovative financial ecosystem, which will be held from 14–21 October 2022.

French fintech companies are also increasingly attracting venture capital investments, which helps them boost their growth. According to France FinTech, there has been an unprecedented year for fintech companies as they raised an aggregate amount of €2,273 million in 93 transactions, compared to €830 million in 2020, which is an increase of around 174 per cent. High-profile deals in 2021 include Sorare (€585 million), Ledger (€380 million), Swile (€176 million), Alan (€185 million), Younited Credit (€142 million) and Lydia (€90 million). The year 2022 has started with the same infatuation with €1,091 million raised in January only in 17 transactions (with Qonto representing €486 million of that amount).

A network of trade organisations (such as France FinTech), incubators, and accelerators, which are often funded by large financial institutions, also supports fintech innovation. The growing interest of these traditional actors is also demonstrated by the acquisitions by large French banks of some of the prominent French fintech companies in the past few years (eg, Shine, Treezor, Budget Insight, Pumpkin).

France's attractiveness is encouraged by various factors, such as the support of regulatory agencies and public authorities to the fintech industry, the quality of French engineers, and the wide network of start-up incubators and accelerators. The French fintech scene covers a wide range of businesses, among which are mobile payments (Lydia, Pumpkin), personal fundraising apps (Leetchi and LePotCommun), neobanks specialised in start-ups and freelancers (Shine, Qonto), crowdlending and crowdfunding platforms (Lendix, KissKissBankBank, Younited, Unilend), robo-advisers (Advize, Yomoni), insurtech (Alan, Akur8) or payroll processors (Payfit).

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 2022, it is not expected that any substantial French legislation related to fintechs will be adopted, especially as legislation is being prepared at the European level. The Digital Finance Package was published by the European Commission on 24 September 2020 and includes (1) a digital finance strategy part and (2) a legislative proposals on the regulation of cryptoassets and the creation of a pilot regime for blockchain-based infrastructures.

Most of the French legislation applicable to financial markets and banking and payment services derives from EU directives or regulations. Three fintech-related reforms, in 2014, 2017 and 2019 are worth recalling.

Both the French government and regulators have proactively supported innovation in financial services in the past few years. The two regulators of the financial sector, the AMF and the ACPR, launched the Fintech Forum in 2016, which is a consultative body where fintech start-ups, financial institutions, experts and regulators can discuss the regulation of financial innovation. In 2016, the AMF and the ACPR also created internal fintech teams, which act as entry points for fintech start-ups that are unsure if the services they are developing require a regulated status. In addition, both regulators have established various fintech-related partnerships with non-EU regulators. The French FinTech Wek is an example, and so is the Paris Blockchain Week Summit (PBWS), hosted for the first time in April 2022. This three-day event was dedicated to blockchain technology and cryptoassets. Changpeng 'CZ' Zhao, CEO and co-founder of Binance, was one of the keynote speaker of the summit. CZ also announced the investment of more than US$100 million in order to create a Web.3 at Station F (Paris), the biggest start-up campus worldwide. Many conferences at the PBWS reaffirmed the goal of turning France into a leading jurisdiction for blockchain technology.

The French government also supports the fintech industry indirectly by drafting tailor-made regulatory regimes for fintech subsectors, such as digital asset service providers, initial coin offerings, and crowdfunding and crowdlending. Some services of the Ministry for the Economy and Finance and the Ministry of Justice also work closely with representatives of the fintech sector.

FINANCIAL REGULATION

Regulatory bodies

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

The Financial Markets Authority (AMF) and the Prudential Supervision and Resolution Authority (ACPR) supervise the financial sector. The AMF

is an independent authority in charge of regulating the financial markets and financial (non-banking) services. The AMF notably regulates asset managers, investment advisers, financial markets infrastructures and digital assets services providers. The task of the AMF is, ultimately, to protect the savings invested in financial products.

The ACPR regulates the banking, payments and insurance sectors. Its goal is to preserve the stability of the financial and banking system. The ACPR is not formally an independent authority, as it is a branch of the French Central Bank. However, in practice, the functioning of the ACPR is very similar to that of the AMF.

Depending on their activities, many large financial institutions are regulated by both the AMF and the ACPR. In addition, the licensing or registration process of certain regulated actors involves an approval from both the AMF and the ACPR, even though only one of them ultimately supervises the regulated entity.

Regulated activities

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

The licensing requirements under French law are very similar to those of other EU countries, since most of French financial and banking law comes from EU directives and regulations. However, some additional licensing requirements apply for categories that have not yet been regulated by the European Union. Providing the following services requires a licence or a registration:

- banking services (ie, granting credits, deposit taking);
- payment services;
- issuing electronic money;
- insurance services;
- managing regulated investment funds;
- investment services, which include advising on investments, transmitting or executing orders on financial instruments, dealing on own account, underwriting and placing of financial instruments, etc;
- operating a financial market infrastructure (such as a trading venue or a central securities depository);
- certain services on digital assets (ie, the custody service, the service of purchasing or selling digital assets against legal currency and, since 9 December 2020, the service of exchanging digital assets for other digital assets and the operation of a digital asset trading platform); and
- operating a crowdfunding or crowdlending platform.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Consumer lending is regulated in France. Essentially, this framework applies to loans of between €200 and €75,000, when such loans are (1) granted to individuals for a purpose unrelated to their commercial or professional activity, and (2) unrelated to a real estate purchase or project. The regulation of consumer lending protects borrowers by compelling lenders to provide them with detailed information, and grant a 14-day cooling-off period to borrowers. The lenders are also required to check the creditworthiness of the borrowers.

Furthermore, French law compels lenders to specify the loan's overall effective rate (TEG) in any written record of the loan and, for consumer loans, prohibit rates from exceeding a legal threshold. Failure to comply with the TEG rules may deprive the lender from its right to receive interest payments, and failure to respect the legal threshold may entail a reduction of the interest rate.

Secondary market loan trading

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

French law does not regulate secondary market loan trading as such. Loan sales must simply comply with the general framework for the assignment of receivables. The assignment must be made in writing and may be done in bulk. The debtors' consent is not required but the transfer cannot be enforced against them unless they have been notified (which is otherwise not mandatory).

A simplified assignment procedure exists for receivables arising from professional loans granted by certain regulated entities (credit institutions, financing companies and some alternative investment funds (AIFs)). Under this procedure, the property transfer is deemed to have occurred on the date that is written on the slip that confirms the transfer, even if it refers to future receivables.

In any case, purchasing an unmatured loan qualifies as a credit operation. Therefore, only certain regulated entities are allowed to purchase such loans. On the other hand, the purchase of matured loans can be carried out by entities subject to little or no regulation.

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 French regulatory regime of collective investment schemes arises from the transposition of the consolidated UCITS Directive (Directive 2009/65/EC of 13 July 2009) and the AIFM Directive (Directive 2011/61/EU of 8 June 2011). The UCITS Directive mainly regulates the management and sale of mutual funds, while the AIFM Directive applies to alternative investment funds, which are mainly dedicated to institutional investors and may invest in illiquid asset classes. Managing a collective investment scheme or an AIF generally requires an asset manager licence, which is granted by the AMF. In addition, most funds also need to be licensed by the AMF before being subscribed by investors.

Various innovative business models have been developed in relation to asset management. Many fintech start-ups have obtained an asset manager licence or collaborated with a licensed asset manager to launch their product. Crowdfunding and crowdlending (or peer-to-peer lending platforms) are subject to a specific regulatory regime in France. Regulation (EU) 2020/1503 on European Crowdfunding Service Providers (ESCP) for business creates a single European statute for all participatory finance activities in the form of securities subscription or loans.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

In France, AIF managers are regulated under the AIFM Directive framework, which means that managing an AIF requires an asset manager licence.

Some fintech start-ups promote or sell to their clients investment opportunities in illiquid assets, such as infrastructure or renewable energy power plants, without being licensed as asset managers. Such activity is risky, since the holding company that raises funds to invest in revenue-generating assets may qualify as a collective investment undertaking, under the meaning of the AIFM Directive. The *Guidelines on the key concepts of the AIFMD* published by the European Securities and Markets Authority in 2013 specifies that an undertaking that satisfies the following conditions is a collective investment undertaking:

1 the undertaking does not have a general commercial or industrial purpose;

2 the undertaking pools together capital raised from investors with a view to generating a pooled return; and
3 the unitholders or shareholders of the undertaking, as a collective group, have no day-to-day discretion or control over the management of the undertaking.

Peer-to-peer and marketplace lending

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

French law regulates peer-to-peer and marketplace lending. Platforms organising such activities must be registered as crowdfunding intermediaries. Crowdfunding and crowdlending platforms have benefited from an ad hoc regulatory regime since 2014, which is currently being regulated. This registration allows these platforms to match borrowers with lenders (which must be individuals), within the limits of €1 million per project and €2,000 per lender and per project (€5,000 per lender and per project if the loans do not bear interest). The maturity of interest-bearing loans cannot exceed seven years.

The crowdfunding intermediary may also be required to obtain another licence (such as a payment institution licence or the status of agent of a payment institution) if other regulated services are provided by the platform.

Crowdfunding

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

Under French law, crowdfunding platforms need to register as crowdfunding intermediaries or crowdfunding advisers, or obtain a status allowing them to provide regulated investment services (such as the investment firm licence) in accordance with the MiFID framework.

Reward-based and donation-based crowdfunding platforms must register as crowdlending intermediaries, while the platforms that offer investments in equities or bonds must register as crowdfunding advisers or obtain an investment firm licence. While the amount that can be raised through crowdlending is capped, the amounts raised through donations are not limited. When a company or an individual raises funds through donations, it may offer rewards to the donors, although there is no obligation to do so.

An equity crowdfunding platform operated by a crowdfunding adviser or an investment service provider can promote offerings of unlisted securities up to an amount of €8 million per project and per year. In theory, the operator of the platform is deemed to provide to its clients investment advice in relation to the securities offered on its platform.

Further licences may also be required if other regulated services are provided by the platform operator, such as payment services.

At the European level, a regulation on crowdfunding service providers entered into force on 10 November 2020 and will supersede the French regime. In France, the new status of European crowdfunding service provider (PSFP) will therefore replace the two current statutes of participatory investment adviser (CIP under AMF control) and participatory finance intermediary (IFP under ACPR control). The current CIP and IFP entities will have 12 months (from November 2021), at least, to comply with the new status. In May 2022, the European Securities and Markets Authority expressed its support for an extension of the transition period (ie, beyond November 2022) to obtain this new European licence. As a matter of conclusion, PSFP status clearly displays a cross-border dimension (as the Regulation on European Crowdfunding Service Providers is European): hence deleting the national regulatory statutes (CIP and IFP or foreign equivalents).

Invoice trading

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

To our knowledge, platforms allowing retail investors to purchase invoices from professionals do not exist in France.

Under French law, various techniques allow companies and freelancers to obtain funds by selling invoices or using them as collateral. These techniques differ in their modalities: in certain cases, such as factoring, the ownership of the invoices is transferred to the factor and the factor is in charge of debt collection, while in other cases, the invoices are used as collateral for a short-term loan and the borrower manages the debt collection.

Generally, all these techniques qualify as credit operations and may only be proceeded by a licensed credit institution or financing company. In addition, the rules applicable to credit operations (eg, the rules related to the effective rate) apply to these financing techniques.

In theory, operating a platform that would act as an intermediary between clients and regulated entities in relation to the sale or use as collateral of invoices would at least require registration as a 'banking operations and payment services intermediary'.

Payment services

12 | Are payment services regulated in your jurisdiction?

France has transposed the Second Payment Services Directive (Directive (EU) 2015/2366 or PSD2), which regulates payment services in the European Union. Under that regulatory framework, credit institutions, payment institutions or electronic money institutions may only provide payment services. Most bank account aggregators and personal finance apps (eg, Bankin', Linxo, Budgea, and Budget Insight) obtained a licence from the ACPR following the adoption of PSD2.

The business model of many fintech start-ups revolves around the provision of payment services. Therefore, these start-ups often choose to collaborate with a payment or electronic money institution, as obtaining such regulated status is costly and burdensome. These start-ups may also provide payment services to their clients by becoming agents of a regulated payment services provider. The registration process of agents with the ACPR is faster and simpler than a payment or electronic money licence application. In addition, agents are subject to limited obligations, since they are deemed to implement the processes and anti-money laundering due diligence measures of their payment services provider. On March 2022, the ACPR published a report to account for the main developments in the sector marked by the emergence of new players – that is, payment and e-money institutions and their agents – that have modernised payment services for the benefit of businesses and individuals. The European Commission is currently organising a public consultation on PSD2, which is expected to end on 2 August 2022.

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?

PSD2 seeks to accelerate the development of online and mobile banking. Many innovative business models developed by fintech start-ups rely on the collection and analysis of data related to the different bank accounts of a single customer (eg, budget apps using account aggregation). Others require some form of access to the infrastructure of the customer's bank (eg, services allowing internet payments without using a credit card, by realising a direct transfer from the customer's bank account to the seller's account).

PSD2 supports these forms of open banking by creating two categories of payment services: the payment initiation service and the account information service. PSD2 also removes certain barriers that prevented third-party providers from obtaining information on their clients' bank accounts.

The Bank of France is also heavily invested in the subject of open banking. On 14 March 2022, it held a seminar on the changes under way in the financial sector, and more specifically those that make it possible to envisage even more accessible, efficient and innovative financial services, while at the same time raising new challenges for both market players and public authorities. The Bank of France has reiterated its commitment to promoting innovation in a framework of trust and has identified three distinct channels: first, at the level of the regulatory framework and as a supervisor; secondly, in the facilitation of private initiatives and the mobilisation of the market; and thirdly, as an operator and actor of 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 are not regulated per se under French law. The services provided by robo-advisers typically fall under a regulated category, whether it is investment advice or portfolio management; therefore, the companies providing these services must be licensed as investment firm or asset managers. Most of the actors providing robo-advice also allow their customers to invest in life insurance policies (which are mainly used, in France, as investment products); such activity is also regulated by the transposition of the Directive on insurance distribution (Directive (EU) 2016/97 of 20 January 2016). Although their business models vary significantly, these companies generally rely on artificial intelligence to suggest an optimal asset allocation, which may vary over time based on the risk profile of the client and their personal savings goals. Most of these robo-advisers are primarily regulated by the AMF as financial investment advisers. Yomoni is also regulated by the ACPR as an insurance broker. Yomoni is the only robo-adviser regulated as an investment management company.

Insurance products

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

The sale and marketing of insurance products is regulated in France, whether the entity providing these products is a fintech start-up or a large financial institution. Some of the largest French fintech start-ups are specialised in innovative insurance products: Alan, which raised more than €300 million over the past three years, including €185 million in April 2021, provides health insurance to freelancers and start-ups; Luko, which raised €20 million in November 2019 and €50 million in December 2020, provides home insurance. Alan obtained an insurance undertaking licence from the ACPR in 2016, while Luko is registered as an insurance intermediary.

In March 2022, France FinTech, in collaboration with Publicis Sapient dedicated a white paper to InsurTech as a player of the digital revolution in financial services. The white paper reminds that the evolutions promised by fintech insurance companies are still to be considered 'risky' due to the structural weaknesses of the sector, which is one of the reasons it is undergoing transformation.

Credit references

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

French law does not regulate the provision of credit references or credit information services. The relevant framework would be the regulation of personal data, namely the General Data Protection Regulation.

CROSS-BORDER REGULATION

Passporting

17 | Can regulated activities be passported into your jurisdiction?

Generally, all activities that are regulated pursuant to an EU directive or regulation may be passported into France, as soon as the entity willing to provide these services in France is regulated in another EU country. Entities licensed in a European Economic Area (EEA) member state may provide regulated services on the territory of another EEA member state either through a branch or subsidiary (freedom of establishment) or directly, without permanent establishment (freedom to provide services). In this way, the regulated entity may either create a French branch and provide services through that branch (freedom of establishment) or provide services to French customers directly, without creating a French branch (freedom to provide services). Today, most French fintech start-ups only address the French market. However, as they grow and raise funds, some of these companies expand into other EU countries. Some regulators worry that the regulatory agencies of these small EU countries may engage in a form of regulatory dumping by offering fintech start-ups a 'fast-track' payment or banking licence. The licensing process of the Bank of Lithuania is reportedly as short as three months, while obtaining the same licence in France may take between six and 12 months.

When a regulated company provides services in France pursuant to the freedom to provide services, no authorisation from the French competent regulator is required. Establishing a French branch does not require an authorisation from the French regulator either, although the home authority of the regulated entity must send a formal notification. However, in both cases, the French regulator may notify the home authority if it considers that the regulated company is breaching its obligations, or take adequate measures if the home authority does not remedy the breach.

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, obtaining a licence in France to provide regulated services involves applying for the licence with a company registered in France. Companies that are regulated to provide these services in another EU country, pursuant to the freedom to provide services, may provide regulated services in France 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?

The sale and marketing of financial services and products in France is subject to the obligations arising from the MiFID framework. Specific restrictions also apply to the distance marketing of consumer financial services, pursuant to the transposition of Directive 2002/65/EC of 23

September 2002. These restrictions include providing information to the consumer prior to the conclusion of the distance contract and a 14-day cooling-off period.

French law also regulates advertising for investment services, and prohibits certain forms of advertising with respect to specific speculative investment products (eg, forex trading platforms, digital assets).

Finally, French law restricts banking and financial solicitation (ie, the unsolicited contact of a person with a view to selling to that person a financial or banking service, or a financial investment). Only regulated entities may use banking and financial solicitation to market their services or products. In addition, certain illiquid or risky investment products may not be marketed using banking and financial solicitation, even by regulated entities. The European Securities and Markets Authority (ESMA), has also issued, in January 2021 a public statement to remind firms of the MiFID II requirements on the provision of investments services to retail or professional clients by firms not established or situated in the EU.

Numerous decisions have been issued following the regulatory restrictions. In its decision of 30 April 2021, the AMF issued a reprimand and a financial penalty of €50,000 to each of the asset management company and its manager. The AMF considered that the company had failed to exercise its activity with the necessary competence, care and diligence in the best interests of its clients, and that the failure was attributable to its manager because of his capacity as manager at the time of the events. On 26 April 2022, the AMF has again sanctioned a financial investment adviser (FIA) and its manager for having sold shares of alternative investment funds (AIFs) under German law that were not authorised for sale in France. The company was therefore reprimanded and fined €150,000. Its manager was banned from exercising the activity of FIA for five years.

CHANGE OF CONTROL

Notification and consent

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

The relevant regulator must usually grant its authorisation before a regulated business changes control.

In particular, the Prudential Supervision and Resolution Authority (ACPR) must grant its prior authorisation before a company takes control of a credit institution, finance company, investment firm, payments institution or electronic money institution. For credit institutions, the ACPR transmits the authorisation request to the European Central Bank, which takes the final decision.

A similar procedure exists for regulated asset managers, with the Financial Markets Authority granting the authorisation.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

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

Fintech companies are required to comply with anti-money laundering (AML) legislation whenever they belong to a regulated category. Most of the categories to which fintech companies belong are subject to AML legislation: credit institutions, payment institutions, electronic money institutions, asset managers, digital assets service providers, insurance undertakings, etc.

Companies issuing tokens pursuant to an initial coin offering (ICO) are subject to AML legislation if they obtained an approval from the Financial Markets Authority (AMF), which is not mandatory. In that case, they are only required to implement AML measures with respect to the amounts raised during the ICO.

Entities providing the following services on digital assets are required to register with the AMF and therefore are subject to AML legislation: the custody service, the service of purchasing or selling digital assets against legal currency; and the service of exchanging digital assets for other digital assets and the operation of a digital asset-trading platform.

Guidance

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

The AMF and the Prudential Supervision and Resolution Authority (ACPR), as well as the European regulatory authorities, regularly publish and update their guidance on anti-money laundering (AML). TRACFIN, the French financial crime unit, also publishes an annual report that outlines the emerging trends in money laundering.

The AMF notes that many regulated fintech companies outsource certain due diligence measures (such as verifications related to asset freezing and politically exposed persons) to a limited pool of providers, which may decrease the global robustness of the AML system. The ACPR warns against the risks incurred by electronic money institutions and payment institutions (which are regulatory statuses often adopted by fintech companies), as well as neobanks. The fact that fintech companies do not physically meet their clients before starting business relationships is a major part of the AML risk identified by the regulators.

Finally, the regulators closely monitor the use of digital assets. TRACFIN started focusing on financial fraud that uses digital assets as early as 2011. The ACPR published new guidelines on 28 January 2022 concerning information on the AML and terrorist financing procedures for digital asset service providers.

In addition, on 31 March 2022, the Chairman of the AMF and the Director of TRACFIN executed a new protocol for the exchange of information and the sharing of expertise between the reference authority for financial regulation and the French Financial Intelligence Unit (FIU) responsible for participating in the fight against money laundering.

This agreement aims to facilitate (1) the traceability and exchange of information between the two partners as well as (2) the sharing of expertise. It provides for the appointment of referents, as well as joint training of regulated persons and the drafting of joint publications such as guides, fact sheets or awareness documents.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Generally, the validity and enforceability of loan agreements and security agreements is subject to the respect of various procedures (eg, prior information of the borrower or the pledgor) or the inclusion of mandatory clauses or elements (eg, the overall effective rate). These requirements depend on the nature of the loan or security agreement and the nature of the parties (ie, loans granted to consumers and securities granted by consumers are subject to stricter requirements).

For example, guarantees granted by natural persons are void if the guarantor has not handwritten in the contract a sentence by which he or she acknowledges that he or she will have to pay in lieu of the debtor. Pledges of receivables may also be void if they are not in written form and they are only enforceable if the transferred debtors have been

notified of the pledge. Regarding loans, French courts consider that the interest rate constitutes a distinct agreement that can be voided separately from the rest of the loan agreement, in which case the legal rate will replace the contractual rate.

As long as these general rules are complied with, French law does not provide specific requirements that may render loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform unenforceable.

Assignment of loans

24 | What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

French law does not regulate specifically the assignment of peer-to-peer or marketplace loans. In addition, a distinction must be made between the assignment of a claim and the assignment of an agreement. Both of these assignments must be done in writing, but a claim can be assigned without the prior consent of the debtor, while the assignment of an agreement requires the prior consent of the other party (which may be given in advance in the agreement). When a claim is assigned without the consent of the debtor, it may only be enforced against it once it has been notified.

Securitisation risk retention requirements

25 | Are securitisation transactions subject to risk retention requirements?

Regulation (EU) 2017/2402 of 12 December 2017 on securitisation applies in France and provides that originators, sponsors or original lenders of securitisations must retain a 5 per cent material net economic interest.

Securitisation confidentiality and data protection requirements

26 | Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

French law does not provide any confidentiality or data protection rules that would be specific to securitisation or to peer-to-peer and marketplace lending. The applicable rules would be those that derive from the General Data Protection Regulation.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

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

The use of artificial intelligence is currently not regulated in France. However, fintech companies using artificial intelligence may be indirectly subject to the regulation protecting personal data (Regulation (EU) 2016/679, also known as the General Data Protection Regulation (GDPR)) if they use personal data as input in their artificial intelligence software.

In any case, the French regulators monitor the increasing use of artificial intelligence by financial institutions. The Prudential Supervision and Resolution Authority (ACPR) published discussion papers on the challenge of artificial intelligence for the financial and the governance of artificial intelligence algorithms in December 2018 and June 2020. The ACPR will watch how these actors use artificial intelligence to make decisions (such as granting a loan or measuring risk). Furthermore, the first Tech Sprint, or regulatory hackathon, organised by the ACPR took place in June and July 2021. It focused on the explicability of artificial intelligence (AI).

Specifically, the challenge was to explain the behaviour of AI-based predictive credit risk models that can only be accessed in a 'black box'. Following the Tech Sprint, the ACPR publishes its report on the major lessons learned, as well as potential future work by the ACPR's Fintech-Innovation Unit. The Tech Sprint has been confirmed again for 2022 and the first part of the year is related to the analysis of the call for applications.

Distributed ledger technology

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

Developing software that runs on a blockchain or a distributed ledger, or participating in a blockchain (by operating a node or broadcasting transactions), is not regulated in France. However, according to the French data protection authority, the GDPR may apply if personal data is uploaded to a blockchain or distributed ledger (eg, when a blockchain is used to timestamp real-world documents, such as a diploma), even though enforcing regulation with respect to public blockchains may be almost impossible. In any case, personal data uploaded to a blockchain should at least be encrypted.

On a different level, one specific use of blockchain technology is regulated under French law. Pursuant to two decrees of December 2017 and December 2018, French companies may use a distributed ledger to issue, register and transfer unlisted securities. These securities registered are legally identical to those registered using a traditional method. The decrees also describe which conditions must be met by the distributed ledger used for such registration (eg, the distributed ledger must allow the identification of the owners of securities). Over the past year, this potential use of blockchain technology has become a major focus of the Financial Markets Authority (AMF), which published a discussion paper on the development of security tokens in March 2020. The AMF recommended to the European Commission that a 'Digital Lab' be created, which would allow national authorities to lift certain obligations arising from EU directives or regulations to promote the development of a security tokens industry.

In this respect, on 24 September 2020, the European Commission published a digital finance package, including a proposal for a regulation on a pilot regime for market infrastructures based on blockchain. The pilot regime aims to create a new regime of exemptions to support the development of financial securities registered in blockchain (security tokens).

In November 2020, the High Legal Committee of the Financial Centre of Paris, a think tank on financial regulation created by the Bank of France and the AMF, published a report on security tokens that makes several recommendations to adapt French law to the use of blockchain as a register for financial securities.

Finally, in April 2021, Societé Générale issued the first structured product in a security token format, which was directly registered on the Tezos blockchain. This transaction follows two issuances of tokenised bonds on the Ethereum blockchain: the Bank of France settled the first one in euros and the second one in central bank digital currency (CBDC). Similarly, Société Générale was involved in the €100 million bond issuance of the European Investment Bank on the Ethereum network.

Cryptoassets

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

The PACTE Act of 22 May 2019 created a regulatory framework for digital assets. The category of 'digital assets' includes cryptocurrencies and ICO tokens, except when such tokens qualify as financial instruments. This category currently includes stablecoins, as long as they do not qualify as electronic money.

The PACTE Act is built around an optional licensing regime: companies providing certain services on digital assets (such as providing investment advice on digital assets or managing a portfolio of digital assets) may apply for an optional licence with the AMF. Obtaining that licence is not mandatory for these actors, but licensed digital asset service providers (DASPs) benefit from a facilitated access to banking services and may advertise their services more broadly than unlicensed DASPs. Licensed DASPs are also subject to anti-money laundering (AML) legislation.

In addition, to comply with the requirements of the Fifth Anti-Money Laundering Directive (Directive (EU) 2018/843 of 30 May 2018), the provision of four categories of digital asset services requires a registration with the AMF as a DASP and are subject to AML legislation. The four categories include (1) the custody of digital assets, (2) the purchase or sale of digital assets against legal currency and, since December 2020, (3) the service of exchanging digital assets for other digital assets, and (4) the operation of a digital asset trading platform.

As of May 2022, there are 37 registered DASPs, including most of the major French digital assets start-ups (Binance, LGO, SheeldMarket, Paymium, Just Mining) and several foreign actors (Bitpanda, Litebit).

At the end of March 2022, the European Parliament voted in favour of the Market in Crypto Assets (MiCA) Regulation, which aims at regulating crypto-currencies and is expected to come into force by the end of 2022. With its proposed regulation on MiCA inspired by the PACTE Act regime and released on 24 September 2020, the European Commission aims therefore to regulate ICOs and DASPs. The proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology aims to create a new regime of exemptions to support the development of financial securities registered in blockchain (security tokens).

The pilot regime provides guidance regarding:

- market infrastructures: multilateral trading platforms and securities settlement systems involved in the exchange of security tokens; and
- operators: MiFID-accredited investment firms, market undertakings and central securities depositories as defined in the Central Securities Depository Regulation.

Another regulation, although not as extensively relayed as the MiCA regulation, was also discussed on 28 April 2022, between European decision makers. The second regulation is known as the Transfer of Funds Regulation (TFR) Directive, which focuses on money laundering on fund transfers. In March 2022, MEPs proposed in their updated version to add the cryptocurrency sector to this directive, which dates from 2015. If this amended version of the directive were to be adopted, it would allow for the monitoring of all cryptocurrency transactions carried out by regulated entities. No updated versions have been circulated since then.

Token issuance

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

Operating a digital asset exchange is included in the list of services on digital assets whose provision require mandatory registration. Companies operating such exchanges may also apply for an optional licence with the AMF.

Licensed digital asset exchanges are subject to a body of rules similar to those of investment firms (eg, information to be provided to customers, own funds requirements, transparency), and to some rules inspired by the regulation of traditional trading venues. On the other hand, exchanges that only obtain a registration are not subject to any specific rule, beyond their duty to implement the AML legislation.

A distinction must be made between platforms that only allow the exchange of digital assets, and those that allow the exchange of digital assets against legal currency. Pursuant to a 2014 position of the ACPR, transferring legal currency from a buyer of digital assets to a seller of digital assets qualifies as a payment service, unless the platform acts as a counterparty for the buyer and the seller. This would mean that no direct contractual relationship is concluded between the buyer and the seller but, rather, the platform buys from the seller and sells to the buyer. Therefore, the operator of a fiat-crypto exchange platform that does not act as a counterparty to the seller and the buyer must obtain a regulated status allowing it to provide payment services, or collaborate with a regulated payment services provider.

DATA PROTECTION AND CYBERSECURITY

Data protection

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

French data protection law mostly derives from the General Data Protection Regulation (GDPR), which is directly applicable in France. There is no specific framework for fintech companies.

Under the GDPR, persons in charge of personal data processing must implement security measures to avoid the personal data files being altered, damaged or accessed by unauthorised third parties.

The amount of stored data must be reduced to the minimum that is necessary to achieve its purpose and it must only be kept for a reasonable duration. While it is being kept, the data must only be accessible to the concerned persons and specific third parties that may be entitled to it by law, such as tax administration.

The persons whose data is collected enjoy specific rights and, in particular, the rights to access, rectify or erase the data. In addition, their consent must normally be obtained before processing their personal data. There are exceptions to this rule, in particular when the data processing is necessary, to perform a contract to which the concerned person is a party.

Cross-border transfers are also regulated. Although exceptions may apply, the general rule is that transfers may only occur to a non-EU country if that country is listed by the European Commission as offering the same degree of protection as exists under the GDPR or if the transfer presents adequate and effectively enforceable guarantees.

While the regulatory stakes are considerable, fintech companies also raise questions about privacy and personal data protection. Indeed, payment data (eg, banking data, purchase data, etc) can allow the tracing of personal activities or the identification of individual behaviour. The anonymity of transactions, international data transfers, legal security in the application of the GDPR, are all key issues in the fintech sector.

Faced with these legal challenges, the CNIL wanted to shed light on the main economic, legal and societal issues surrounding data and payment methods, in the form of a white paper, published last October 2021 and entitled 'When trust pays off: today's and tomorrow's payment methods and the challenge of data protection'. The white paper was intended for both (1) the general public (for a better understanding of the privacy issues related to data and payment methods) and (2) professionals (for developments on the CNIL's points of vigilance in this area, as well as the priorities it wishes to set in terms of support). It aims at reviewing the CNIL's legal points of vigilance regarding the application of the GDPR in the field of payments and outlines the work to be done to support professionals in this field. The CNIL's goal is to contribute to the competitive equality between players as well as to the perfect compliance of these players with the GDPR.

The CNIL's approach is not only informative. In December 2021, the CNIL fined the French fintech Slimplay (founded in 2009) €180,000 for having left the bank data of 12 million people unprotected on a server for more than four years.

The ACPR has also published, in July 2021, a special guide on IT risk management for companies in the banking, payment services and payment and investment services investment services following the new provisions relating to IT risk management introduced by the amending Order of 25 February 2021.

Cybersecurity

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

France has transposed Directive 2016/1148 of 6 July 2016 (the Network and Information Security Directive), which provides a legal framework for cybersecurity. Under that regulation, operators of essential services must notify the French Cybersecurity Agency of any breach or security incident.

The list of operators of essential services includes most regulated financial institutions: banks, financial markets infrastructures, payment and electronic money institutions, etc. Therefore, fintech companies would be subject to this regulatory framework if they belong to one of these categories.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

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

Financial services companies may outsource material aspects of their business, provided that they remain fully responsible for the functions or activities that have been outsourced. They must also implement measures to monitor the compliance of their contractor with applicable regulations. Additionally, the outsourcing of material functions or activities must be notified to the regulator.

In a statement dated July 2021, the Prudential Supervision and Resolution Authority (ACPR) reminded stakeholders several of their obligations. This statement follows the context of increase use of external service providers for the execution of services. Those services often imply heavy prudential regulations. The ACPR has therefore reminded the stakeholders it supervises of their obligations in this area and particularly the need for them to control substantially the services they have chosen to services they have chosen to outsource.

Cloud computing

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

The French and EU regulatory authorities increasingly monitor the use of cloud computing in the banking, insurance and payment sectors. The regulators have noticed that large institutions and start-ups heavily rely on large-scale cloud computing providers (eg, Amazon, Google and Microsoft).

In 2017, the European Banking Authority (EBA) published its recommendations on outsourcing to cloud service providers, which were later included in its guidelines on outsourcing arrangements. The Prudential Supervision and Resolution Authority complies with these guidelines. The guidelines require regulated institutions to include in their agreements with cloud service providers various provisions related to audit rights and reporting obligations. However, the large-scale cloud service providers seem unwilling to include such provisions in their agreements, which may force the French or European authorities to draft a regulation imposing the inclusion of standard contractual provisions in these agreements.

In May 2021, the High Legal Committee of the Financial Centre of Paris published a report on the banking cloud. The report follows the launch of a working group, in February 2020, whose objective was to analyse this phenomenon with respect to the current architecture of the rules applicable to the banking sector in terms of prudential and supervisory rules.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

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

Under French law, software may be protected through both patent protection and copyright.

Copyright protection does not require taking any specific steps. As long as the piece of work is original, protection would be automatically granted from the creation of the software and for a duration of at least 70 years after its author passes away. Regarding software, this protection may concern the computer program as such, as well as its user interface, its name, its user guide and preliminary works such as prototypes. Where copyright protection applies, the author enjoys a set of rights over the piece of work, which they may decide to transfer in part or completely. In particular, those include an exclusive right to publish the software, to be quoted as its author and to exploit it.

Any kind of invention may be patented, including those that are implemented through software, as long as the invention is new, relates to a patentable subject matter (from which business methods and computer programs are excluded), is susceptible of industrial application and involves an inventive activity (ie, is not obvious). Patents remain valid for 20 years following their filing.

It is also possible to register the name of a software as a trademark. Trademarks grant specific protection as to business use, for an indefinitely renewable period of 10 years after their filing.

IP developed by employees and contractors

36 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?

French law divides intellectual property into three distinct areas: (1) copyrights, (2) trademarks and (3) patents. This scission obviously leads to different legal regimes.

Under French law, and as applicable to copyrights, new intellectual property developed by employees and contractors belongs to them. They may sell their rights to their employer, but French law also prohibits the blanket sale of future intellectual property rights. French courts have accepted, however, that the sale can be organised in advance in the contract of employment and then formalised once a year in a document listing each individual creation of the employee that is concerned by the transfer. In principle, they must receive an additional remuneration independently from their salary. The legal regime applicable to copyrights contains exceptions, in particular regarding software development.

Unless provided otherwise in the contract, as long as they were developed in the course of the employees' functions or following the instructions of the employer, intellectual property rights over software and their documentation are deemed to be automatically transferred to the employer. However, the employee still keeps certain 'moral' intellectual property rights, which mainly comprise the right to oppose modifications that would be detrimental to the developer's honour or reputation. As for collective works, which are works that are not attributable to the same person, they are automatically owned by the company.

Finally, for patents, there is a specific regime provided under French law. French IP law provides that an invention made by an employee during his or her employment contract belongs to the employer if the employee has an inventive mission, as described in the French Intellectual Property Code. In this way, depending on the nature of the employee's work, the patent may belong to the employer or to the employee. Thus, there is a stronger right of preference to the company for an R&D engineer rather than a lawyer, whose mission is not to invent anything.

Joint ownership

37 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 relation to copyrights and trademarks, French law provides that joint authors must exercise their intellectual property rights by mutual agreement. Civil courts may intervene in case of conflict.

They may, however, exercise their intellectual property rights alone if their respective contributions can be identified and distinguished as being of different kinds. In such a case, they must make sure not to prejudice the exploitation of the joint work.

On the other hand, as far as patents are concerned, a particular regime should be applied. In any case, it can be organised by a co-ownership regulation on a trademark or a patent. This legal scheme is very frequent.

Trade secrets

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

Under French law, a piece of information may be protected as a trade secret if:

1 it is not generally known or easily accessible to people who are used to dealing with such information owing to their profession;
2 its secrecy confers commercial value to it; and
3 the legitimate holder of the piece of information has undertaken reasonable steps to maintain its secrecy.

Unauthorised or dishonest procurement, unauthorised use or unauthorised divulgation of such trade secrets constitutes an infringement. The procurement, use or divulgation of a trade secret for anyone who knows or ought to know that they had obtained the secret from someone who was unlawfully using or divulgating it also constitutes an infringement. However, there are derogations for journalists and whistle-blowers, for whom the protection of legitimate interests is recognised by French or EU law, and for employees and their representatives acting in the course of their legitimate functions.

Available remedies include damages, as well as injunctions and other measures aimed at stopping, evidencing or preventing the infraction from happening.

During civil or commercial court proceedings, judges may resort to certain measures aimed at protecting the confidentiality of trade secrets in relation to the procedure. This includes, for instance, the possibility for judges to read certain documents on their own or to adapt the content and publicity of their decision. Such measures are only available if they represent the only way to protect the secret and if they do not prejudice the rights of the defence.

Branding

39 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 be protected under design or trademark protection or copyrights.

Designs and models protection may be awarded to the appearance of any product or part thereof, provided that the product is an industrial or artisanal object, which includes parts designed to be assembled into a complex product, packaging, presentations, graphic symbols and typefaces, but excludes computer programs. The patent designs must be new (ie, no identical or similar designs or models has already been registered), proper (ie, the overall visual impression it creates for the informed observer differs from that produced by any already disclosed design) and consistent with public order and decency.

Design protection requires registration, which is effective for a five-year duration. Registration may be renewed for five years at a time, up to an overall maximum of 25 years. It should be further noted that there exists an unregistered design regime and its protection is available under EU law.

Design protection prohibits any unauthorised manufacture, offer, launch, import, export, transhipment, use or possession for those purposes of a product incorporating the design. Any infringement constitutes counterfeiting and incurs the civil liability of the author of the act. In addition to damages, right holders may obtain specific measures and remedies seeking to prevent, evidence or stop the infraction. Knowingly committing such counterfeiting also constitutes a criminal offence.

Rights granted by design protection cannot be enforced in certain situations. Those include, in particular:

1 acts performed for private and non-commercial purposes;
2 acts performed for experimental purposes; and
3 acts of reproduction for purposes of illustration or teaching, if such acts mention the registration and the name of the owner of the rights, are in accordance with fair commercial practice and do not prejudice the normal exploitation of the design.

The National Institute of Industrial Property's (INPI) national database for patent designs or lawyers or trademark attorneys with the help of

specialised service providers can help companies ensure that their designs do not overlap with registered models or patent designs.

Trademark protection may be awarded to 'signs' serving to distinguish the goods or services of a person from those of another person. Such signs must comply with certain requirements. For instance, they must be capable of being represented in the national register of trademarks in such a way as to enable any person to determine precisely and clearly the subject matter of the protection granted to their owner.

Trademark protection requires the registration of the design, which is effective for a 10-year period that can be renewed an indefinite amount of times.

Trademark protection grants property rights over the trademark in relation to the products or services for which it was registered. Essentially, it prohibits unauthorised commercial use of the sign or of similar signs in relation to services or products that are identical or similar to those for which it was registered. Most infringements to trademark protection constitute counterfeiting, In addition to damages, right holders may obtain specific measures and remedies seeking to prevent, evidence or stop the infraction. Under certain circumstances, this form of counterfeiting may also constitute a criminal offence.

The INPI's national database for trademarks or lawyers/trademark attorneys with the help of specialised service providers can help companies search for existing trademarks and avoid infringements.

Remedies for infringement of IP

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

Infringement of intellectual property rights may give rise to damages. The rise of damages could be (1) civil penalties (damages), (2) criminal remedies, and (3) custom remedies.

In addition, French law also allows various additional remedies, such as injunctions, that aim to prevent, evidence or stop intellectual property rights infringement. The particulars of those remedies vary depending on the kind of intellectual property right that is at stake.

It should be noted that an action very specific to the French system is (1) seizure proceedings including, among others, the seizure of data, and (2) ex parte proceedings allowing to raise the defendant's promises to obtain evidence of the infringement.

COMPETITION

Sector-specific issues

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

At the time of writing, there do not seem to be any specific competition law issues regarding fintech companies. However, the French Competition Authority is currently conducting research on the fintech sector. This initiative may unveil issues or spark changes to French legislation in the future.

In an opinion about the challenges of fintech published in April 2021, the French Competition Authority expressed its concerns about the strengthening of the market power of BigTech (ie, GAFAM and BATX). Indeed, the data massively collected by BigTechs gives them an undeniable competitive advantage in that it allows them to reinforce the attractiveness of their platforms at lower cost.

TAX

Incentives

42 | 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 benefit from various tax credits depending on their size and the exact nature of their activity:

- a 'research' tax credit may be awarded to companies of any size that have R&D activities in the European Economic Area. The credit amounts to 30 per cent of the R&D expenditures but is reduced to 5 per cent for their portion exceeding €100 million (tax credit can be refunded in cash if unused in most situations); and
- an 'innovation' tax credit may be awarded to small and medium-sized companies. Those companies must not have more than 250 employees, a turnover of less than €50 million or a balance sheet total of less than €43 million. The credit concerns expenditures not already covered by the 'research' tax credit that relate to the design of prototypes or pilot installations of new products. It amounts to 20 per cent of those expenditures, which are capped at €400,000 per year. It is possible to request the immediate refund of the credit. This credit may disappear in 2023.

Fintech start-ups may also benefit from the 'young innovative company' status. This status is open to independent companies that have been in existence for less than eight years, and the conditions related to the number of employees, turnover and balance sheet total are the same as those for the 'innovation' tax credit. This status allows them to benefit from several tax incentives, including important company tax exonerations for a period of two years.

Small fintech companies may benefit from reduced corporate income tax rates, provided their turnover is less than €7.63 million and their capital has been fully paid up and is at least 75 per cent owned by individuals (or by a company applying this criterion). In such case, they enjoy a 15 per cent company tax rate on the first €38,120 of their profits. Fintech start-ups may also benefit from (1) a favourable and well-established immigration regime to attract talent; (2) the French stock option regime for newly created companies (BSPCE) and competitive RSU/free shares plans; and (3) a clear legal environment, which includes the recently issued VAT guidelines that offer more comfort on VAT treatment for most fintech companies.

Increased tax burden

43 | 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 French Parliament adopted a 'GAFAM' digital tax in 2019. This tax is equal to 3 per cent of the revenues from taxable digital services provided in France by eligible entities. However, it applies to large French or foreign companies whose revenues exceed €750 million worldwide and €25 million in France. Any excess GAFAM tax may be credited over the minimum taxation on multinational once and if implemented.

IMMIGRATION

Sector-specific schemes

44 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?

France has created the 'Talent Passport' residency permit programme to attract skilled professionals, researchers, entrepreneurs, investors and artists. This permit grants these persons a four-year renewable residency permit.

There is no specific programme for the technology or financial sectors.

UPDATE AND TRENDS

Current developments

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

The most notable recent development of the regulation of the fintech sector is the publication by the European Commission on 24 September 2020 of a digital finance package, including a digital finance strategy and legislative proposals on cryptoassets (proposal for a Regulation on Markets in Cryptoassets (MiCA) and proposal for a regulation on a pilot regime for market infrastructures based on blockchain (Pilot Regime)) and digital resilience.

As mentioned above, the Transfer of Funds Regulation (TFR) is also at a decisive moment in its negotiation. In March 2022, MEPs added the cryptocurrency sector to this directive, which dates from 2015. More precisely, on 31 March 2022, it is two new amendments, which were voted for by the European Parliament Economic and Monetary Affairs (ECON) Committee and the Committee on Civil Liberties (LIBE) of the European Parliament regarding the TFR Directive. The two amendments officially aim at limiting money laundering, by requiring companies to identify the senders and recipients of their transfers, without minimum value limits (even when a private portfolio is involved). By adding the cryptocurrency sector to this directive, which originally dates from 2015, the monitoring of all cryptocurrency transactions carried out by regulated entities is allowed. While the European Parliament's version published at the end of March 2022 was deemed very restrictive for crypto-asset providers, trialogues between the European Parliament, the European Commission and the European Council on the TFR have been ongoing since 28 April 2022.

KRAMER LEVIN

Hubert de Vauplane
hdevauplane@kramerlevin.com

Judith Smadja
jsmadja@kramerlevin.com

47 avenue Hoche
75008 Paris
France
Tel: +33 01 44 09 46 00
www.kramerlevin.com

Germany

Christopher Götz, Elmar Weinand, Felix Biedermann, Jochen Kindermann, Martin Gramsch, Sascha Kuhn and Lena Menger

Simmons & Simmons

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 getting 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 recognise that in particular in the crypto sphere many of the traditional players now jump on this trend as well. The gap between traditional and new players in this respect became smaller, which is in line with the approach that BaFin always took (i.e., 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. The Federal Financial Supervisory Authority (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 FinTechRat includes experts appointed by the German Ministry of Finance who support the legislature in developing a suitable regulatory framework. All German cities that are hubs for fintech (Berlin, Frankfurt, Munich and Hamburg) offer additional support through fintech centres. In addition, universities in or around fintech centres tend support and dedicate resources to the development of an effective fintech ecosystem.

FINANCIAL REGULATION

Regulatory bodies

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

The Federal Financial Supervisory Authority (BaFin) is responsible for regulating fintech products and services in Germany if they fall under the scope of regulated activities or products. A fintech company may be subject to reduced requirements provided it limits its activities to, broadly:

- the distribution of open or closed-end funds registered for public distribution in Germany; or
- the distribution of participation rights, subordinated loans or profit participation rights.

In these cases, the local trade office would be the competent supervisory authority.

Regulated activities

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

Pursuant to section 32(1), sentence 1 of the German Banking Act (KWG), anyone wishing to conduct banking business or to provide financial 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 or financial services is set out in section 1(1) and (1a) KWG and includes, among other things:

- the acceptance of monies from the public (deposit business);
- the provision of money loans (lending business);
- the brokering of business involving the purchase and sale of financial instruments (investment broking);
- providing customers or their representatives with personal recommendations in respect of transactions relating to certain financial instruments where the recommendation is based on an evaluation of the investor's personal circumstances or is presented as being suitable for the investor and is not provided exclusively via information distribution channels or for the general public (investment advice);
- the purchase and sale of financial instruments on behalf of and for the account of others (contract broking);
- the management of individual portfolios of financial instruments for others on a discretionary basis (portfolio management);
- dealing in foreign notes and coins (foreign currency dealing);
- the ongoing purchase of receivables on the basis of standard agreements, with or without recourse (factoring);

- the conclusion of financial lease agreements in the capacity of the lessor and the management of asset-leasing special purpose vehicles (financial leasing); and
- the purchase and sale of financial instruments separately from the management of a collective investment scheme for a community of investors, who are natural persons, on a discretionary basis with regard to the choice of financial instruments (asset management).

Since the beginning of 2020, 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 the Directive 2014/65/EU on markets in financial instruments or Annex I of Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms. The provision of payment services is licensable based on the provisions of the German Act on the Supervision of Payment Services (ZAG).

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 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 Law 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 (GewO) and, therefore, the operation of a P2P lending platform could trigger the requirement for a loan broker licence.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

Managers of alternative investment funds located in Germany are regulated under the KAGB. The same also applies to a certain extent to German branches of non-German managers of alternative investment funds. Alternative investment funds may only be marketed in Germany once they are registered or passported for distribution to investors in Germany. Germany has implemented the Alternative Investment Fund Managers Directive 2011/61/EU.

Depending on the nature of their actual activities, fintech companies could fall outside the scope of the KAGB if their activities do not constitute 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.

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 each 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.

Peer-to-peer 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 GewO may be required.

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 and rewards-based crowdfunding, which is also referred to as crowd sponsoring;
- loan-based crowdfunding (crowd lending); and
- crowd investing.

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.

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 the Payment Services Directive 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 ZAG and comprises the same activities set out in the Payment Services Directive.

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 banking (eg, KWG and the German Securities Trading Act) and commercial law (eg, GewO). 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 broking. 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 the EU Credit Rating Agency Regulation 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 on markets in financial instruments. Providing false or misleading information is generally prohibited. Further rules apply for specific types of financial instruments like investment funds.

CHANGE OF CONTROL

Notification and consent

20 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

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

Firstly, a distinction must be made between anti-corruption and bribery (ABC) regulations and rules for combating money laundering (AML).

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 the 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 to 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 the German Money Laundering Act (see section 2), 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.

There have been some important changes to the Money Laundering Act in the past: on 1 January 2020, the Act was amended to implement the requirements of EU's Fifth Anti-money Laundering Directive. The changes imposed additional obligations, especially for regulated financial services businesses, including fintech companies. Since this date, 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 anti-money laundering regulations, including internal communication of policies and procedures; and
- report suspicious transactions.

Furthermore, the abovementioned amendment of the Money Laundering Act includes unified, enhanced due diligence requirements for transactions with high-risk countries and extended data access competencies for the Federal Financial Intelligence Unit and law enforcement agencies. In addition, digital companies will be 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. Furthermore, 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 for bribery. At a state level, some German federal states already have 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 been debating for years whether companies should be held liable under a kind of criminal law (ie, corporate sanctions law) if its responsible persons commit crimes or regulatory offences. The current federal government is working on such an act but it remains to be seen when and with which exact requirements such new legislation will enter into force.

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. After all, the risk for the company is always the same in the event of infringement as very high fines are threatened.

Guidance

22 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 to repeat 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, in addition, should comply with all applicable anti-financial crime guidance for the financial sector.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

There is no special legislation applicable in Germany in relation to peer-to-peer (P2P) lending (ie, the general regulatory and civil law provisions are applicable). A distinction needs to be made between direct and indirect P2P lending.

- In relation to direct P2P lending, the agreement is concluded directly between the investor and the borrower. However, owing to regulatory limitations (ie, licence requirements for lending activity), this structure is not popular in Germany.
- In relation to indirect P2P lending (which is more common in Germany), a cooperating licensed bank is involved. The licensed bank enters into a loan agreement with the borrower. Once the loan agreement between the bank and the borrower has been entered into, the bank assigns under a purchase and assignment agreement its claims under the loan agreement pro rata to the respective investor whereby often an affiliated company (intermediary) of the platform provider is interposed. Thus, there is no direct agreement between the borrower and the investor. The bank cooperates with the platform provider under a cooperation agreement and the platform provider serves as loan broker under a loan brokerage agreement with the borrower. For the loan brokerage, the platform provider needs permission according to the German Industrial Code. Further, the platform provider must not receive monies that are determined to have been forwarded, otherwise a payment services licence could be required. Generally, care should be taken in the documentation that the purchase of claims does not qualify as factoring, that the money laundering requirements have been complied with and that the borrower consents to the transfer of the borrower's personal data to the investors.

With regard to loan agreements with consumers, consumer protection laws need to be taken into account (ie, special information and form requirements as well as revocation rights are applicable). If consumer information undertakings are not complied with, this can give rise to damage claims by the borrower; if the form requirements are not complied with, the loan agreement can be void; or if the consumer has not been instructed correctly on his or her revocation rights, the loan can become revocable for an indefinite period. With regard to formal requirements for the execution of the loan and security agreements, written form is required; electronic form is permitted as well, except for in the case of certain security documents where a notarisation by a German notary is required (eg, land charge deeds, which include an immediate enforcement clause or share pledge agreements, which relate to the pledge of shares in a German limited liability company).

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

An assignment agreement would need to be concluded in relation to the assignment of the loan claims; there are no further perfection requirements and the borrower's consent is not required. The assignment is also valid if it is not being disclosed to the borrowers. In the case of a transfer of rights and obligations under a loan agreement (ie, transfer of the whole contractual relationship) to a new lender of record, the borrower (as both debtor and creditor of the transferred rights and obligations) would need to consent to the transfer. Usually, the loan documentation would include provisions requiring the prior consent of the borrower to such a transfer. In the case of an assignment of rights under a loan agreement, an assignment is generally possible without the consent of the borrower. If an assignment of the rights under a loan agreement was explicitly excluded by a borrower in the loan documentation, the assignment would be void. However, in the case of the indirect P2P lending structure, the loan documentation should already include the prior consent of the borrower to transfer the rights and obligations under the loan agreement to the investor (or intermediary, as the case may be).

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

Regulation (EU) 2017/2402 provides for the general securitisation framework, including rules regarding risk retention. Under this framework, the originator, sponsor or original lender of a securitisation must retain a material net economic interest in the securitisation of not less than 5 per cent. However, if securitisation is achieved via an intermediary single purpose company, this entity will no longer be allowed to retain risk as the originator. Rather, this may only be done by an originator with a broader business purpose, the sponsor or the original lender. The required entity must possess sufficient substance to hold the assets for a minimum period of time before they are securitised. Furthermore, assets to be securitised must not be selected with the aim of rendering the losses on such assets higher than the losses on comparable assets remaining on the balance sheet of the originator without disclosing this accordingly to investors.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

Yes, the special purpose company would be subject to data protection laws regarding information relating to the borrowers. However, in the case of the indirect P2P lending structure, the loan documentation

should already include the consent of the borrower to share its information with the special purpose company.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 | 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 by 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 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 German Banking Act (KWG)), 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 accurateness 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 seqq and 362 et seqq EU 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, KWG 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 broking. 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.

Distributed ledger technology

28 | 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, 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 the European Market Infrastructure Regulation (EU) No 648/2012 (EMIR), the Markets in Financial Instruments Regulation (EU) No 600/2014 (MiFIR), the Central Securities Depositaries Regulation (EU) No 909/2014, the Markets in Financial Instruments Directive II 2014/65/ EU, the Alternative Investment Fund Managers Directive 2011/61/EU and the Securities Financing Transactions Regulation (EU) 2015/2365 as well as the national implementation thereto must be regarded. For instance, a use case involving the clearing of assets by deploying DLT would have to fulfil the requirements of EMIR and MiFIR regarding authorisation and regulated entities. BaFin has the power to prohibit unauthorised businesses. In addition, smart contracts and initial coin offerings (ICOs) are currently under close scrutiny by the supervisory authorities.

BaFin issued a consumer warning with regards to risks associated with ICOs on 15 November 2017. Specific risks identified by BaFin include the significant price fluctuations of tokens and, in many cases, a lack of information regarding ICO providers making ICO businesses prone to the risk of fraud, money laundering and the financing of terrorism. BaFin also published an advisory letter to the classification of tokens on 20 February 2018. The key aspect of this letter is that BaFin will assess on a case-by-case basis whether a token constitutes a financial instrument, a security or a capital investment. The supervisory classification of a token determines the applicability of the existing legal framework, the services and products associated with the tokens. Depending on the classification of tokens, several legislative acts apply including, among others, the WpHG, the German Securities Prospectus Act, the German Capital Investment Act, the German Capital Investment Code and the KWG. Further, at the beginning of 2020 crypto-custody business was added to the list of licensable activities.

Cryptoassets

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

Yes. BaFin treats bitcoin and other crypto-tokens as a financial instrument in the form of 'units of account'. These units of account are similar to foreign currencies and are not legal tender. Bitcoin is neither central bank money nor e-money under German law: it is not central money because it is not issued by the central bank, and it is not e-money because it is not issued by an issuer against whom a claim can be established. The distribution of bitcoin 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.

At the beginning of 2020, crypto-custody business was 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).

Token issuance

30 | 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 special legal regime for digital currency exchanges or brokerages in Germany. The German regulator assesses activities in the context of cryptocurrencies or tokens on a case-by-case basis. It has been BaFin's administrative practice for several years now to view bitcoin and similar cryptocurrencies as financial instruments in the form of units of account. Consequently, the rules for dealings with financial instruments apply. In a guidance note dated 20 February 2018, BaFin states that the mining of cryptocurrencies and the sale of the mined tokens are, in principle, licence-free in Germany. However, persons who, for example, buy and sell cryptocurrencies in their own name and for the account of others on a commercial scale are likely to conduct the licensable business of financial brokerage. Further, operating a digital currency exchange could qualify as operating a multilateral trading facility. Additionally, operators of mining pools may be carrying on licensable activities.

DATA PROTECTION AND CYBERSECURITY

Data protection

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

In 2018, the EU General Data Regulation (GDPR) came into force with direct effect across the EU. 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 members of the EEA 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 EEA, 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 *Schrems II* CJEU decision. 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 EEA 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 in order 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, a new Federal Data Protection Act (BDSG) came into force at the same time as the GDPR. The BDSG makes use of opening clauses, such as for the processing of personal data in the context of employment and for the appointment of data protection officers. The oversight of 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

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

'Fintech' here is understood 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 (ie, BaFin Circular 10/2017 on Banking Supervisory Requirements for IT), the Insurance Supervision Act (ie, BaFin Circular 10/2018 on Insurance Supervisory Requirements for IT) and German Capital Investment Code (ie, BaFin Circular 11/2019 on Capital Management Supervisory Requirements for IT).

Regarding obligations to report serious payment security incidents under the Payment Services Directive 2 (PSD 2, implemented in Germany by the Payment Services Supervision Act (ZAG)), BaFin has set out guidance in its Circular 08/2018 (BA) for reporting serious payment security incidents (effective until 30 September 2022) and in its 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 namely 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), 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 on the financial markets are, thus, also regulated as operators of a critical infrastructure or digital service, or both, under the German IT Security Act (IT-SiG). 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 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 BSI Act). The same accounts for critical service providers in terms of IT security and network security (see section 8c 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 latest amendments of the IT-SiG, BSI is furnished with information and audit rights. Furthermore, 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

33 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 services companies. Section 25b of the German Banking Act (KWG) sets the framework and the Federal Financial Supervisory Authority's (BaFin) publication 'Minimum Requirements for Risk Management' (MaRisk) further details the requirements for outsourcing in chapter AT9. Further, BaFin indicates that the 'Guidelines on Outsourcing' published by the European Banking Authority (the EBA-Guidelines on Outsourcing) are also relevant for 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

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

Sections 25a paragraph 1 and 25b KWG stipulate 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. New guidance on the 'Bank regulatory requirements relating to IT' was published by BaFin. 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.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

35 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 EPO Boards of Appeal provide useful guidance in this respect.

IP developed by employees and contractors

36 | 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, 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, which 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 R&D 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 to moral rights will remain with the creator of such software.

Joint ownership

37 | 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

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

Germany implemented the Trade Secrets Directive (EU) 2016/943 on 26 April 2019 with the civil law on the protection of trade secrets (ie, the German Trade Secrets Act), which first and foremost protects trade secrets. 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 German Trade Secrets Act protects information that meets all 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 debated requirement is the trade secret measures implemented by the trade secret owner. The adequacy of the measures depends on the company and the usual confidentiality measures, the value and nature of the trade secret in detail as well as the specific circumstances of its use. Physical access restrictions and precautions as well as contractual security mechanisms should be considered.

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 (ie, 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 in order 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 in order to facilitate the enforcement of trade secret rights.

Nevertheless, a key take away is that trade secrets should firstly 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.

Branding

39 | 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 a European trademark. Furthermore, 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

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

There are various measures against infringements of intellectual property 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 intellectual property 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

41 | 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 abusive behaviour of strong market players primarily directed at the 'GAFAs' (Google, Amazon, Facebook, Apple). 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 Google, Facebook and Amazon. 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 finance 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 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 also catch highly valued start-up fintech companies if the target company did not 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 of the thresholds will mean that fewer transactions are subject to merger control proceedings.

The financial sector has also seen enforcement actions. 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 number in independent online payment procedures to infringe competition law in order 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 the revised Payment Services Directive (Directive (EU) 2015/2366) (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 (P2P 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 or 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. This topic remains on the agenda of the FCO as well as other authorities.

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 the 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 ensured also in the future and the transaction could be cleared.

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.

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.

Lastly, the German Federal Government revised its foreign direct investment regime several times in reaction to the covid-19 outbreak. 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

42 | 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 the European 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. Furthermore, 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 (ie, 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 (ie, 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 the EU or an 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 has, 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 (ie, taxpayers with profits of not more than €200,000 (before considering an investment deduction amount according to section 7g (1) sentence 1 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.
- Furthermore, 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 carry forwards. However, tax loss carry forwards (as well as interest carry forwards) 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

43 | 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

44 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 EU 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 EU 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 an EU Blue Card can obtain a national visa for an entry in advance at the relevant German diplomatic mission. This visa will be replaced by an EU Blue Card after entry by the relevant immigration authority.

To obtain an EU 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 €56,400 gross per year (for 2022; the threshold differs annually) is required. For shortage occupations, the minimum annual gross salary is €43,992 (for 2022). Shortage occupations are, inter alia, natural scientists, mathematicians, architects, engineers, engineering scientists and academic specialists in information and communication technology. If those requirements are met, no approval of the employment agency is necessary.

After a residence of 33 months in Germany, holders of a EU 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.

Since 1 March 2020, skilled workers have had 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-member countries outside of the EU. 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 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 for 'shortage professions' in the past.

In comparison to the EU 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.

For applicants without a university degree who have completed professional training, a temporary residence permit can be applied for if the applicant gets a position in a shortage occupation. This applies for positions as an expert in IT system analysis, IT sales and an expert in software development and programming. 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 a labour market examination that is less comprehensive than the Federal Employment Agency. A priority examination is not required.

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; that at least 60 months of compulsory contributions to the statutory pension insurance have been made; that the applicant has sufficient German language skills; that he or she has basic knowledge of the legal and social order as well as living conditions in Germany; that a permit for employment is available; that no reasons of public safety and order speak against the residence; and that sufficient housing space is available for the applicant and, as the case may be, for family members.

simmons +simmons

Christopher Götz
christopher.goetz@simmons-simmons.com

Elmar Weinand
elmar.weinand@simmons-simmons.com

Felix Biedermann
felix.biedermann@simmons-simmons.com

Jochen Kindermann
jochen.kindermann@simmons-simmons.com

Martin Gramsch
martin.gramsch@simmons-simmons.com

Sascha Kuhn
sascha.kuhn@simmons-simmons.com

Lena Menger
lena.menger@simmons-simmons.com

MesseTurm
Friedrich-Ebert-Anlage 49
60308 Frankfurt
Germany
Tel: +49 69 90 74 54 0
Fax: +49 69 90 74 54 54
www.simmons-simmons.com

UPDATE AND TRENDS

Current developments

45 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.

Hong Kong

Donia Chu, Jolyon Ellwood-Russell, Michelle Ta and Ian Wood

Simmons & Simmons

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 600 fintech companies and start-ups, covering services in the areas of payment, AI, 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 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 issued revised guidance on this in January 2022 (replacing the 2018 guidance). The HKMA has issued a Fintech 2025 strategy to drive fintech development in Hong Kong, including 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.

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 government as a priority investment area.

A range of Hong Kong Government Funding Support programs 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, SM 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, are 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 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 licence 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; and
- Type 10: providing credit rating services.

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 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.

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 and 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.

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.

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 of 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?

No. However, the HKMA published the Open Application Programming Interface (API) Framework for the Hong Kong Banking Sector in July 2018. This is intended to encourage 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. Phase III and IV of the API Framework was due to commence progressively from December 2021. Of the 28 participating banks, 22 retail banks are due to launch Phase III by the end of June 2022 and a number of banks with corporate and SME offerings having launched or are due to launch Phase III in the course of 2022. All 28 participating banks are due to launch Phase IV (comprising faster payment services app-to-app payments) in 2022.

In November 2020, the HKMA announced that it is exploring a new data strategy and considering building a new financial infrastructure called the Commercial Data Interchange (CDI). The CDI will enable a secure and efficient data flow between banks and sources of commercial data. The HMKA is conducting a proof-of-concept study in collaboration with banks. In December 2021, the HKMA issued a call to banks and data providers to actively participate and connect into the CDI for risk management, with a statement that banks with a material SME financing business are expected to join the CDI by the end of 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.

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.

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, 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, a new Hong Kong credit reference platform (CRP) is due to launch by the end of 2022. In December 2021, the HKMA issued a circular to banks asking them to prepare for the CRP. Additional codes of practice and a revised supervisory policy manual from the HKMA on consumer credit data are expected in the course of 2022.

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?

It is unlikely that the SFC 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.

CHANGE OF CONTROL

Notification and consent

20 | 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. 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

21 | 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.

The Hong Kong government is proposing to adopt changes to the anti-money laundering legislation in Hong Kong to require exchanges trading virtual assets (including cryptocurrencies) to apply for a licence from the SFC and to carry out customer due diligence in respect of anyone trading on the exchange.

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

22 | 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.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

A loan agreement does not need to be executed as a deed and, accordingly, in respect of a Hong Kong company entering into a loan agreement, only the signature of the persons acting upon the company's authority (eg, the persons authorised in the board resolutions to sign) is required (under section 121 of the Companies Ordinance).

A security agreement would typically be required to be executed as a deed. As such, in respect of the execution by a Hong Kong company, the deed should be executed either with the common seal affixed in accordance with the requirements in the articles of association of the company or, in accordance with the Companies Ordinance, without the common seal affixed but signed by, in the case of a Hong Kong company with two or more directors, any two directors or any director and the company secretary or, in the case of a Hong Kong company with sole director, its sole director.

The key risk in respect of a peer-to-peer (P2P) marketplace lending platform is that in respect of pure P2P lending involving companies or individuals lending via the lending platform, each such lending company and individual may be regarded as carrying on a business as a money-lender and, thus, is subject to licensing and regulatory restrictions, including the restrictions on the form of loan agreement, early payment,

interest rate, moneylending advertisements and duty to provide information and so on under the Money Lenders Ordinance.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

According to the Hong Kong Law Amendment and Reform (Consolidation) Ordinance, the legal assignment of a loan by the assignor (ie, the lender) to the assignee (ie, the purchaser) will be perfected if:

- the assignor absolutely assigns the receivable to the assignee;
- the assignment is in writing and signed by the assignor in favour of the assignee; and
- a written notice of assignment is delivered to and received by the party liable to pay the loan (the underlying debtor, in other words, the borrower).

Regarding the written notice of assignment above, although there is no time limit within which this notice of assignment has to be given, the notice should be given as soon as possible to complete the perfection of the assignment.

If the assignment is not perfected, the assignment concerned may still constitute an equitable assignment (in contrast to a legal assignment), which is still recognised by the Hong Kong courts, although there are some practical disadvantages that may affect enforcement.

The lender (as assignor) need not obtain the consent of the borrower unless the loan agreement between the lender and the borrower contains a prohibition on the lender assigning certain or all of its rights under the loan agreement to a third party.

Notification to the borrower of the assignment is not mandatory for the assignment to be effective. However, there are a number of practical and legal difficulties that arise from an assignment without notice to the debtor (that is, an equitable assignment rather than a legal assignment).

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

In June 2016, the Hong Kong Monetary Authority (HKMA) published the Credit Risk Transfer Activities Module (the CRTA Module) for inclusion in the HKMA Supervisory Policy Manual. The CRTA Module defines an 'originator' as:

- a person who directly or indirectly originates the underlying exposures in a securitisation transaction; or
- in relation to a securitisation transaction for which underlying exposures are acquired from third-party entities, a person who serves as a sponsor of the transaction by establishing, managing and advising on the transaction or by providing any credit enhancement or liquidity facility in respect of the transaction.

While there are no detailed risk retention requirements imposed on originators, the CRTA Module provides that an originating authorised institution should ensure that investors have readily available access to all materially relevant data concerning the transaction, including, where relevant and appropriate, the amount of risk retention by the authorised institution in the transaction and the manner in which the risk is retained.

The CRTA Module also provides that an authorised institution acting as an originator of a securitisation transaction should be prepared to explain to the HKMA the possible impacts on its financial position, capital adequacy, liquidity and asset quality, with regard to the risks incurred by it in the structure of the transaction including through retention of the first-loss tranche or provision of liquidity facilities.

The CRTA Module states that unless otherwise agreed with the HKMA, an authorised institution should refrain from investing in, or incurring an exposure to, a securitisation if the originator has not disclosed its compliance with any risk retention requirements applicable to it (in any jurisdiction).

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

The Personal Data (Privacy) Ordinance governs the collection, use and dissemination of the personal data of living individuals.

Data about or provided by obligors may also be protected by more general Hong Kong legal and regulatory principles that require the protection of confidential information. Largely, these apply irrespective of the legal structure of the obligor, but their precise application depends on the circumstances.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 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 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 HKMA has also issued guidance on the use of 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 using big data and artificial intelligence.

Distributed ledger technology

28 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

29 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).

New laws governing the licensing and AML obligations of virtual asset service providers (VASPs) are also expected to come into effect in 2022.

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 SFC. Additional requirements apply to companies engaged in distribution funds that invest in virtual assets.

The promotion and sale or trading of cryptoassets that constitute a security (which includes derivatives or futures contracts relating to digital currencies such as bitcoin) is a regulated activity and requires a licence.

Token issuance

30 | 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 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.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 | 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.

- DPP1: 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.
- DPP2: 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.
- DPP3: 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.
- DPP4: data users must take all practicable steps to ensure that personal data is protected against unauthorised or accidental accessing, processing, loss or erasure.
- DPP5: 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.
- DPP6: 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 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

32 | 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

33 | 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

34 | 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

35 | 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 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 UK and the European Patent Office (where the UK is designated). They have a maximum period of protection of 20 years from the filing date of the designated application.

IP developed by employees and contractors

36 | 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
- 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

37 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). 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 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 (in each case, subject to any other agreement reached between the co-owners).

Trade secrets

38 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

39 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 of the internet for any unregistered trademark rights that may prevent use of the proposed mark.

Remedies for infringement of IP

40 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

41 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

42 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

43 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

44 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 three 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 the Technology Talent Admission Scheme, 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.

UPDATE AND TRENDS

Current developments

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

There is a particular focus on opening up banking and payment infrastructure and services in Hong Kong and the roll-out of services by the holders of the virtual bank licences.

The Hong Kong Monetary Authority (HKMA) is seeking to improve the flow of financial information through the establishment of the Commercial Data Interchange and the Credit Reference Platform. It is also exploring the use of central bank digital currencies to ease cross-border trade settlement, in particular the testing of e-CNY and e-HKD. In 2017, the HKMA began exploring the use of wholesale central bank digital currency on the mBridge platform, an initiative to explore cross-border payment use cases between the central banks of China, Hong Kong, Thailand and the United Arab Emirates. In addition, in April 2022, the HKMA issued a discussion paper to gather feedback on the feasibility of a retail e-HKD.

The government is seeking to establish qualifications and competency standards for the fintech sector. It was announced in the government's 2021 Policy Address and 2022–2023 Budget that the development of recognised professional qualification standards for sector practitioners under the Qualifications Framework for Fintech was underway. In December 2021, the HKMA launched the Enhanced Competency Framework on Fintech with the aim of establishing competency standards for fintech practitioners in the financial services industry.

The government is likely to introduce legislation to regulate cryptocurrency exchanges and to require them to hold a licence to operate and to restrict their services to professional investors.

Donia Chu
donia.chu@simmons-simmons.com

Jolyon Ellwood-Russell
jolyon.ellwood-russell@simmons-simmons.com

Michelle Ta
michelle.ta@simmons-simmons.com

Ian Wood
ian.wood@simmons-simmons.com

30th Floor, One Taikoo Place
979 King's Road
Hong Kong
China
Tel: +852 2868 1131
Fax: +852 2810 5040
www.simmons-simmons.com

Indonesia

Winnie Yamashita Rolindrawan and Ruth Margaretha Ginting

SSEK Legal Consultants

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

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

Similar to last year, the use of fintech by Indonesian consumers continues to increase, with no signs of slowing down. Many potential new players are considering, or are in the process of, entering the Indonesian market. Areas of particular interest include investment, payment systems, digital banking and cryptocurrency trading. The Indonesian government 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. To cite just one example, in the cryptocurrency sector, the Indonesian government has committed to establishing a cryptocurrency futures exchange by the end of 2022, which in turn has encouraged more cryptocurrency traders to expedite their investment plans in Indonesia.

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, with the support of the Indonesian central bank, Bank Indonesia (BI) and the Financial Services Authority (OJK) as the main authorities regulating the fintech sector, has 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. One example of this is the sandbox regulations issued by the OJK and BI to keep 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 between 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 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 also to strategise expediting the digitalisation of the financial services industry and pushing economic recovery.

The Indonesian government also attempts to balance support for fintech development and innovation with the protection of Indonesian consumers and the public. As part of this balancing act, the government, through the OJK, recently issued OJK Regulation No. 6/POJK.07/022 regarding the Protection of Consumers and the Public in the Financial Services Sector, dated 18 April 2022. This regulation provides more robust and specific protections for consumers who use services or goods in the financial services sector.

FINANCIAL REGULATION

Regulatory bodies

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

Fintech products and services in Indonesia are mainly regulated by two government bodies, Bank Indonesia (BI) and the Financial Services Authority (OJK).

Regulated activities

4 Which activities trigger a licensing requirement in your jurisdiction?

Generally, all parties that conduct business activities in Indonesia are subject to licensing and registration requirements under the authority of the Ministry of Investment / Indonesian Investment Coordinating Board. For businesses in the financial sector, there are additional specific licensing requirements under the authority of BI or the OJK.

For business activities that fall under the authority of BI, such as payment systems, whether the licensing requirement is 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 the pre-transaction or post-transaction steps will be deemed as supporting providers, which does not trigger any licensing requirement from BI. The same applies to business activities that fall under the authority of OJK and whether they will trigger a licensing requirement.

For financial services regulated under OJK Regulation No. 13/POJK.02/2018 regarding Digital Financial Innovation in the Financial Services Sector, dated 16 August 2018, the following activities are subject to licensing requirements in Indonesia:

- transaction settlement: this focuses on, among other things, investment settlement;
- capital raising, such as equity crowdfunding, virtual exchange, smart contracts and alternative due diligence;
- investment management; for example, advanced algorithms, cloud computing, capability sharing, open-source information technology, automated advice and management, social trading and retail algorithmic trading;
- fundraising and fund disbursement: this includes activities such as peer-to-peer lending, alternative adjudication and third-party application programming interface;
- provision of insurance; for example, sharing economy, autonomous vehicles, digital distribution and securitisation and hedge funds;

- market support; for example, artificial intelligence or machine learning, machine-readable news, big data, social sentiment, market information platforms and automated data collection and analysis;
- other digital finance supporting activities, such as social and eco-crowdfunding, Islamic digital financing, e-waqf, e-zakat, robo-advisers and credit scoring; and
- other financial services activities; for example, invoice trading, vouchers and products using blockchain-based applications.

Foreign organisers of trade through an electronic systems provider (PPMSE), 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. However, we note that as of this writing, the relevant regulatory authority does not yet have in place the necessary licensing infrastructure for foreign PPMSE.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Consumer lending is regulated in Indonesia, with a particular focus on information technology-based money lending services (peer-to-peer lending), as regulated under OJK Regulation No. 77/POJK.01/2016 regarding Information Technology-Based Money Lending Services, dated 29 December 2016, as amended by OJK Regulation No. 4/POJK.05/2021 of 2021 regarding Application of Risk Management During the Use of Information Technology by Non-Bank Financial Service Institutions, dated 17 March 2021. 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. A company that wishes to register with the OJK is required to have a minimum issued and paid-up capital of 1 billion Indonesian rupiahs (about US$70,000). However, the current minimum issued and paid-up capital for foreign investment companies is at least 10 billion Indonesian rupiahs (about US$700,000). If this minimum issued and paid-up threshold is not met, there is a risk that licensing applications will not be approved.

Once an applicant is registered, he or she will have one year to apply for a licence from the OJK. A company engaging in the provision of peer-to-peer lending is not allowed to engage in any other business activities. The regulation refers to information technology-based money lending services (peer-to-peer lending) as the provision of financial services that allow the lender to meet the borrower in the framework of entering into a lending agreement in rupiah directly through an electronic system by using the internet. However, to date, there is a moratorium in effect on the issuance of new peer-to-peer licences in Indonesia. While this moratorium is in effect, the OJK is focusing on expediting the licensing process for existing peer-to-peer players in Indonesia while improving the relevant peer-to-peer regulatory framework. At the end of January 2022, the OJK issued a statement that it would soon issue a regulation in the non-bank financial sector amending fintech peer-to-peer lending regulations. The amendment is said to include provisions on ownership of joint funding service platforms, consumer protection prohibitions, restrictions on controlling ownership of fintech companies, minimum paid-up capital, minimum equity and maximum funding. We expect that by the time the anticipated peer-to-peer regulation is issued that the government will also end the moratorium on the issuance of new peer-to-peer licences.

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.

The prevailing regulations do not expressly categorise activities into collective investment schemes and there is no specific regulation on collective investment schemes. Instead, the Indonesian government provides regulations with respect to alternative finance products such as equity crowdfunding platforms and peer-to-peer lending, both of which are under the authority and supervision of the OJK. Peer-to-peer lending is described as an information technology-based money lending service, which is specifically regulated under a different regulation than equity crowdfunding. Equity crowdfunding is regulated under the auspices of the OJK, through 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. The OJK has the authority to regulate, register and issue licences, as well as supervise equity crowdfunding activities. For example, for certain equity crowdfunding business actors, the OJK not only requires a licence but also an additional certificate from Indonesia's Ministry of Communication and Informatics evidencing ESP certification.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

There is no regulation that specifically regulates the managers of alternative investment funds. However, in general, investment managers are regulated under the authority of the OJK, pursuant to OJK Regulation No. 24/POJK.04/2014 of 2014 regarding Implementation Guidelines for the Functions of Investment Managers, dated 19 November 2014.

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. 77/POJK.01/2016 regarding Information Technology-Based Money Lending Services, dated 29 December 2016, as amended by OJK Regulation No. 4/POJK.05/2021 of 2021 regarding Application of Risk Management During the Use of Information Technology by Non-Bank Financial Service Institutions, dated 17 March 2021. 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 the framework of entering into a lending agreement in rupiah directly through an electronic system by using the internet.

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 access for issuers (Indonesian limited liability companies) 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, Bank Indonesia (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 (PBI 22/23), dated 30 December 2020, 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, and BI Regulation No. 23/7/PBI/2021 regarding Payment System Infrastructure Providers, dated 1 July 2021. 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?

To date, there is no law or regulation that requires financial institutions to make customer or product data available to third parties to promote competition, unless to the relevant government agency for supervision purposes or for law enforcement purposes.

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-advisers or other companies that provide retail customers with automated access to investment products in Indonesia. However, a definition of robo-advisor is provided in the elucidation of 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 definition, a robo-advisor is an information technology-based investment management service that provides automatic portfolio management based on an algorithm to assist investors in managing their finances and investments without the involvement of a human investment manager.

The general rules regarding licensing for investment advisors are found in the Decision of Head of the Financial Institutions Supervisory Agency (Bapepam) No. Kep-26/PM/1996, which has not yet been revoked although Bapepam is already non-existent and its tasks and authorities taken over by the OJK. In practice, as far as we are aware, only one company with a robo-advisor platform has successfully been licensed by the OJK as an investment advisor.

Insurance products

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

In principle, the selling and marketing of insurance products in Indonesia is regulated and licensed by the OJK, although there seems to be no differentiation yet between fintech companies and companies that engage in the conventional selling and marketing of insurance products. 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.

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 Financial Services Authority (OJK). A credit report is defined under OJK Regulation 5/POJK.03/2022 regarding Credit Information Management Agencies, dated 28 March 2022, and BI Circular Letter No. 15/49/DPKL regarding Credit Information Management Agencies, dated 5 December 2013 (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. The credit report generated by the 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 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.

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 fulfil 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.

CHANGE OF CONTROL

Notification and consent

20 | 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, Bank Indonesia, or the Financial Services Authority if a change of control occurs. There are certain sectors that only require 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

21 | 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 procedures and also need to conform to anti-bribery regulations in Indonesia. Players in the cryptocurrency sector in Indonesia, including cryptocurrency traders and futures exchanges, are also required to have in place anti-money laundering procedures and prevention of terrorism funding and proliferation of mass destruction weapons guidelines, pursuant to the Commodity Futures Trading Regulatory Agency (Bappebti) Regulation No. 8 of 2021 regarding Guidelines for the Implementation of Physical Market of Crypto Assets in Futures Exchange, dated 29 October 2021. Bappebti requires companies at least to have internal guidelines before they obtain a registration certificate operating licence from Bappepti. However, initial coin offering and initial token offerings activities are not yet clearly regulated in Indonesia and are not subject to this Bappebti regulation.

Guidance

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

Currently, there is no specific regulatory or industry anti-financial crime guidance for fintech companies. However, the Financial Services Authority (OJK) has issued a regulation for anti-money laundering and prevention of terrorism financing programmes in the financial services sector in general, which includes fintech companies. This regulation is OJK Regulation No. 12/POJK.01/2017 of 2017, dated 21 March 2017, which was last amended by OJK Regulation No. 23/POJK.01/2019 of 2019, dated 30 September 2019.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Loan agreements in a peer-to-peer lending platform are acknowledged and regulated. Based on Financial Services Authority (OJK) Regulation No. 77/POJK.01/2016 regarding Information Technology-Based Money Lending Services, dated 29 December 2016, as amended by OJK Regulation No. 4/POJK.05/2021 of 2021 regarding Application of Risk

Management During the Use of Information Technology by Non-Bank Financial Service Institution, dated 17 March 2021, there are two agreements in a peer-to-peer lending scheme:

- an agreement between the provider of the peer-to-peer lending service (the provider of the platform) and the lender; and
- an agreement between the lender and the borrower.

The agreement on the provision of peer-to-peer lending between a provider and a lender is made in electronic document format and must include, at least, the:

- agreement number;
- date of the agreement;
- identities of the parties;
- provisions on the rights and obligations of the parties;
- amount of the loan;
- interest rate of the loan;
- amount of commission;
- tenor;
- breakdown of relevant expenses;
- provisions on fines (if any);
- mechanism of dispute settlement; and
- settlement mechanism if the provider is unable to continue its operational activities.

The provider is required to provide the lender with access to information on the appropriation of funds. This information does not include information related to the identity of the borrower. The information will include, at least, the:

- amount of loaned funds to the borrower;
- purpose of the use of the funds by the borrower;
- amount of the loan interest; and
- tenor of the loan.

The lending agreement between the lender and borrower is made in electronic document format and must include, at least, the:

- agreement number;
- date of the agreement;
- identities of the parties;
- provisions on the rights and obligations of the parties;
- amount of the loan;
- interest rate of the loan;
- instalment value;
- tenor;
- object of guarantee (if any);
- breakdown of relevant expenses;
- provisions on fines (if any); and
- mechanism of dispute settlement.

The provider is required to provide the borrower with access to information on the position of the received loan. This information will not include information related to the identity of the lender. The agreements above are made by using electronic signatures in accordance with the prevailing laws and regulations on electronic signatures. If the provider uses a standard agreement (for any agreement between the provider and the users of the platform, be it lenders or borrowers), the standard agreement must not:

- transfer the responsibilities or obligations of the provider to the user; or
- state that the user is subject to new regulations, addendums, supplementary or amendments drawn up unilaterally by the provider within the period during which the user uses the service.

A standard agreement or standard clause is described as a written agreement as set forth unilaterally by the provider and that contains standard clauses regarding content, format, as well as the method of production, and is used to make a mass offer of service to users.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

Presently, there is no specific fintech law or regulation that addresses the assignment of loans on a peer-to-peer lending platform. Given this absence, the assignment of loans should be allowed under the freedom of contract principle contained in the Indonesian civil law code. Any assignment of a loan will need notification to the borrower.

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

This is not specifically regulated under the prevailing laws and regulations in Indonesia.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

This is not specifically regulated under the prevailing laws and regulations. However, there is a general regulation regarding the protection of personal data in electronic systems, namely, Minister of Communication and Informatics Regulation No. 20 of 2016 regarding Personal Data Protection in Electronic Systems, dated 1 December 2016. In this case, information relating to the borrowers is protected with respect to the process of obtaining, collecting, processing, analysing, storing, displaying, disseminating, providing access to and destroying the borrowers' data. As such, if the special purpose company used to purchase and securitise peer-to-peer or marketplace loans used an electronic system to conduct its business, it will be subject to the duty of confidentiality or data protection laws regarding information relating to borrowers under the above regulation.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 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, including robo-advice. However, robo-advice is mentioned as an example of an information technology-based supporter of crowdfunding services, along with blockchain, aggregators and big data analytics, pursuant to Financial Services Authority (OJK) Regulation No. 57/POJK.04/2020 regarding Information Technology Based Crowdfunding Services, dated 11 December 2020, as amended by OJK Regulation No. 16/POJK.04/2021, dated 26 August 2021.

Distributed ledger technology

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

There is no specific rule or regulation governing the use of distributed ledger technology or blockchains. However, blockchain and distributed ledger technology are referred to in the elucidation of OJK Regulation No. 57/POJK.04/2020 regarding Securities Offerings Through Information Technology-Based Crowdfunding Services (Securities Crowdfunding), dated 11 December 2020, as amended by OJK Regulation No. 16/POJK.04/2021 dated 26 August 2021. This regulation defines blockchain as the service of bookkeeping in an information technology-based financial transaction that records and stores transaction evidence or a distributed ledger through a computer network, whether private or public. The regulation does not provide any definition for a distributed ledge.

Cryptoassets

29 | 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 no specific regulation in Indonesia that governs the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and NFTs. The most relevant regulation, Commodity Futures Trading Regulatory Agency (Bappebti) Regulation No. 8 of 2021 regarding Guidelines for the Implementation of Physical Market of Crypto Assets in Futures Exchange, dated 29 October 2021, does not specifically govern the promotion or use of cryptoassets, including digital currencies, stablecoins, utility tokens and NFTs. However, the definition of 'cryptoassets' under this regulation is very broad.

Under the regulation above, cryptoassets are deemed commodities that can be traded in a cryptoasset exchange. The regulations describe cryptoassets as intangible commodities in the form of digital assets, using cryptography, peer-to-peer networks and distributed ledgers to manage the creation of new units, verify transactions and secure transactions without any intervention by other parties. In Indonesia, cryptoassets or cryptocurrencies are not recognised as payment instruments and, therefore, are prohibited from being used as payment instruments.

Token issuance

30 | 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, to date, no specific regulation governing ICOs or initial token offerings (ITOs) in Indonesia. Commodity Futures Trading Regulatory Agency (Bappebti) Regulation No. 8 of 2021, which is the main regulation for cryptoassets, explicitly states that it does not regulate ICOs or ITOs.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 | 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 transfer are:

- 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
- Minister of Communication and Informatics Regulation No. 20 of 2016 regarding Personal Data Protection in Electronic Systems, dated 1 December 2016.

Cybersecurity

32 | 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. 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. Fintech companies may be subject to the provision 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

33 | 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.

Cloud computing

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

There is no specific legal requirement or regulatory guidance with respect to the use of cloud computing in the financial services industry. However, cloud computing is generally regulated under Minister 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

35 | 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

36 | 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 employees or contractors or consultants, 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

37 | 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

38 | 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

39 | 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, 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

40 | 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

41 | 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

42 | 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 investors.

Increased tax burden

43 | 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. 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 for cryptocurrency trade transactions, MOF Regulation No. 68/PMK.03/2022 regarding Value Added Tax and Income Tax on Crypto Asset Trade Transactions. VAT in the amount of 0.1 per cent will be imposed if the crypto trader is registered as a trade 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 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 Spotify and Netflix that operate outside of Indonesia with a significant number of users in the country.

IMMIGRATION

Sector-specific schemes

44 | 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, and, therefore, 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 foreign workers, as set out by the Ministry of Manpower.

UPDATE AND TRENDS

Current developments

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

We understand that a Financial Services Authority (OJK) moratorium on the registration and licensing of peer-to-peer lending companies in Indonesia is still in effect, so the OJK will, for the time being, no longer accept registration applications. There has been no confirmation on how long the moratorium will last, but the OJK has hinted that it will end soon. We also understand that the OJK is preparing a new regulation on collective funding services based on information technology that would replace the current regulation on peer-to-peer lending, namely OJK Regulation No. 77/POJK.01/2016 regarding Information Technology-Based Money Lending Services, dated 29 December 2016. Although the new regulation had been expected to be issued in the second semester of 2021, it has as not yet been issued as of this writing.

There are also ongoing discussions of a draft Personal Data Protection Law, but it is not clear when the law might be passed by the House of Representatives and issued by the government.

Winnie Yamashita Rolindrawan
winnierolindrawan@ssek.com

Ruth Margaretha Ginting
ruthginting@ssek.com

Mayapada Tower I, 14th Floor
Jalan Jend. Sudirman Kav 28
Jakarta, 12920
Indonesia
Tel: +62 21 521 2038 / +62 21 2953 2000
www.ssek.com

Ireland

Joe Beashel and Ian O'Mara

Matheson

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 EU via a UK payments or e-money licence have sought to obtain authorisation by the Central Bank of Ireland (the Central Bank) so as 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 May 2022, 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 (NDRC) 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. European 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 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, 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 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 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 (MiFID II) was transposed into Irish law by the European Union (Markets in Financial Instruments) Regulations 2017 (the Irish MiFID II Regulations). Engaging in any of the investment services and activities listed in MiFID II (eg, providing investment advice or executing client orders) is a regulated activity requiring authorisation. Other parts of the MiFID II package also have direct effect in Ireland.

Engaging in 'banking business' requires authorisation under the Central Bank Act 1971. The European Union (Capital Requirements) Regulations 2014 transposed the Capital Requirements Directive 2013/36/EU (CRD IV) into Irish law and the requirements for obtaining an Irish banking licence are based on the transposition of the CRD IV package. Other parts of the CRD IV package also have 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 Central Bank Act 1971.

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. Commencement of the new legislation is likely to occur during the summer of 2022.

Multiple aspects of consumer lending are also regulated (at a 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 as amended, and Directive 2008/48/EC.

The Central Bank's Consumer Protection Code 2012 and associated addenda (the CPC) 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 KYC, to establish the suitability of the product, and adhere to lending and advertisement requirements.

There are also separate requirements for mortgage lending to consumers, including the 'housing loan' requirements under the Consumer Credit Act 1995, European Union (Consumer Mortgage Credit Agreements) Regulations 2016, implementing the provisions of Directive 2014/17/EU 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 SMEs. 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 the Alternative Investment Fund Managers Directive 2011/61/EU (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 or marketplace lending in Ireland. Some of the regimes described in this chapter (eg, retail credit, the new 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.

Regulation (EU) 2020/1503 (the Crowdfunding Regulation) and Directive (EU) 2020/1504 (the MiFID II 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 II Amending Directive into national law. European crowdfunding service providers (ECSPs) are excluded from MiFID II by the MiFID II Amending Directive, and ECSPs are instead covered by the Crowdfunding Regulation.

The Crowdfunding Regulation applies to peer-to-peer 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 II 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 its 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, small and medium-sized 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 2015/2366/EU (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 'money transmission business'. Money transmission business is defined as a business that comprises or includes providing a money transmission service to members of the public.

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 (ie, 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 the Insurance Distribution Directive (EU) 2016/97 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/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, 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's 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.

CHANGE OF CONTROL

Notification and consent

20 | 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 relevant competent authority. For firms authorised in Ireland, the notification is made to 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

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

The Criminal Justice (Corruption Offences) Act 2018 (the Act) 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.

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, 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.

The EU's Fifth AML 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 the Payment Services Directive II), 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

22 | 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 2015/2366/EU (PSD2) and other specific regimes, as applicable. In June 2021, the Central Bank issued anti-money laundering and countering the financing of terrorism 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.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

For a loan agreement or security agreement to be binding, there must be an offer, acceptance, consideration or intention to create legal relations and certainty as to terms. The application of these principles does not depend on the particular technology that is being used so that acceptance can be evidenced by clicking in a designated box on a peer-to-peer or marketplace lending platform website.

There are additional requirements for specific types of loan agreement, for example under the European Communities (Consumer Credit Agreements) Regulations 2010, the Consumer Credit Act and the European Union (Consumer Mortgage Credit Agreements) Regulations 2016.

A deed is necessary for certain types of transactions, including property-related transactions. Deeds made by individuals must be signed, and Irish law recognises electronic contracts and signatures in accordance with the requirements of the Electronic Commerce Act 2000 and Regulation 910/2014 on electronic identification and trust services for electronic transactions.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

There are two main types of assignments of legal rights under Irish law: a legal assignment and an equitable assignment. Irish law is similar to English law in this regard. The distinction can be important at point of enforcement and in general terms, a legal assignment is preferable. To create a legal assignment of a debt, the assignment must be in writing and signed by the assignor; the assignment must be absolute, in other words, unconditional and not merely by way of security; and express notice in writing must be given to the borrower from whom the assignor would have been entitled to receive the debt. Part of a debt, or other legal chose in action, may not be legally assigned; only the whole debt may be legally assigned.

The Central Bank's Consumer Protection Code 2012 and associated addenda (the CPC) requires a regulated entity to provide two months' notice before transferring any part of its regulated activities (including loans) to a third party. This obligation only applies to a regulated entity that would include regulated lenders and also regulated credit servicing firms appointed to hold the legal title to, or service, the loans. Assuming there is no prohibition on assignment without the consent of the borrower under the terms of the loan, Irish law would not otherwise require the borrower to be informed of the assignment. However, any such assignment without notice would take effect as an equitable assignment (see above).

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

The Securitisation Regulation (Regulation EU 2017/2402), which became directly applicable across the EU on 1 January 2019, applies in Ireland. It requires institutional investors to ensure that the originator, sponsor or original lender of a securitisation retains at least a 5 per cent net economic interest in the securitisation.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

Where the special purpose vehicle is established in Ireland and controls personal data, it will be subject to the full scope of Ireland's data processing laws. Irish incorporated companies, partnerships or other unincorporated associations formed under the law of Ireland, and persons not falling within the forgoing but who maintain in Ireland an office, branch or agency, or a regular practice will be established in Ireland for these purposes. Data controllers that make use of equipment in Ireland for processing data can also fall within the scope of Ireland's data processing laws in certain circumstances. Broader confidentiality provisions applicable to a special purpose vehicle would typically arise as a matter of contract, and the implied banker's duty of confidentiality at common law is unlikely to apply.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 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, 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 has issued a discussion paper relating to the impact of such innovation on its Central Bank's Consumer Protection Code 2012 and associated addenda (the CPC) and the delivery of financial services to consumers in Ireland.

Distributed ledger technology

28 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 has issued a discussion paper relating to the impact of such innovation on its CPC and the delivery of financial services to consumers in Ireland.

Cryptoassets

29 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 AML and CTF purposes following the EU's Fifth Anti-Money Laundering Directive. Assuming the cryptoassets are not 'financial instruments' or other form of collective investment, there is no regulatory framework governing cryptoassets in Ireland outside of the current AML framework.

However, there are plans ahead at EU level for a Markets in Crypto-Asset Regulation (or 'MiCA', similar to MiFID II) 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 is expected to be finalised at EU level during the course of 2022.

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 crypto-asset service provider whenever the EU's MiCA legislation is finalised.

Token issuance

30 | 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.

DATA PROTECTION AND CYBERSECURITY

Data protection

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

The General Data Protection Directive (Regulation 2016/679) (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 EU 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

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

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 relevant European Supervisory Guidelines 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 PSD2 and other specific regimes, as applicable).

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

33 | 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 the MiFID II and 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 takes an active interest in compliance by regulated firms with outsourcing requirements and in November 2018, published a 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

34 | 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

35 | 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

36 | 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.

Joint ownership

37 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

38 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 the Trade Secrets Directive 2016/43 into Irish law and provide for civil redress measures in respect of the unlawful acquisition, use and disclose 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

39 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 EU (as an EU trademark) or internationally. Trade and service mark rights give registered owners certain rights to prevent others 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

40 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

41 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

42 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 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 R&D expenditure carried on within the EEA. 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 OECD's 'modified nexus' standard. This can reduce the rate of Irish corporation tax to 6.25 per cent for profits derived from certain IP 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 (EII) and Start-up Refunds for Entrepreneurs (SURE) 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 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

43 | 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 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.

IMMIGRATION

Sector-specific schemes

44 | 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 business, or the technology and financial sectors, in Ireland. The ordinary rules in relation to employment permit requirements apply.

UPDATE AND TRENDS

Current developments

45 | 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 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.

Joe Beashel
joe.beashel@matheson.com

Ian O'Mara
ian.o'mara@matheson.com

70 Sir John Rogerson's Quay
Dublin 2
Ireland
Tel: +353 1 232 2000
www.matheson.com

Japan

Ken Kawai, Akihito Miyake, Tomoyuki Tanaka, Yutaka Shimoo and Kensuke Inoue

Anderson Mōri & Tomotsune

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 non-fungible tokens' sector, digital securities' sector and buy now, pay later (BNPL) services.

Non-fungible token- (NFT) related businesses became popular, especially in the online gaming sector. In addition, content holders, digital-art artists and advertising agencies have rushed to this new market.

In 2021, digital security businesses have been gaining stronger momentum. Their main focus is on digital corporate notes and tokenised equity interests of real estate funds.

Among mobile payment services, BNPL services have been growing rapidly in tandem with the development of this business abroad. It is notable that PayPal acquired Paidy Inc, one of the largest BNPL services providers in Japan, last autumn to expand its BNPL services to Japan.

Additionally, on 1 November 2021, the Act on Provision of Financial Services came into effect enabling the establishment of financial services intermediary businesses that are capable of intermediating the cross-sectoral banking, securities and insurance financial services under a single licence.

In June 2022, the bill to amend the Payment Services Act (PSA) 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 amended Acts will come into force within one year. The amended PSA will introduce licence obligation

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.

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 the 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 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). A company that provides its users with the following services is required to undergo registration as a Crypto Asset Exchange Services Provider:

1 the sale and purchase of CAs in exchange for fiat currencies or the exchange of CAs for other CAs;
2 intermediary, agency or delegation services in respect of the acts listed in item (1);
3 management of customers' money in connection with the acts listed in items (1) and (2); or
4 management of CAs for the benefit of another person (namely, a crypto-asset custody service).

Fiat-backed stablecoin issuers and intermediaries will be subject to licensing requirements from the second quarter of next year.

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 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.

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.

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.

CHANGE OF CONTROL

Notification and consent

20 | 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

21 | 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 transaction, occupation and, in the case of a corporate customer, 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

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

No.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

In terms of a peer-to-peer or marketplace lending platform in Japan, it had been construed that each lending participant would be required to be registered as a moneylender under the Moneylending Business Act unless there were multiple anonymised borrowing participants. However, the Financial Services Agency published its interpretation that each lending participant is not required to be so registered if:

- all the borrowing participants are corporations;
- the platform is formed as a *tokumei kumiai*, which is an agreement under the Commercial Code to be entered between the platform operator registered as a moneylender and each lending participant; and
- the agreement prohibits each lending participant from contacting any borrowing participants for the purpose of collecting money.

In terms of enforceability of loans, the portion of any interests (including lending-related fees) exceeding 15 per cent or higher (or up to 20 per cent) of the loan principal amount shall be null and void under the Interest Rate Restriction Act.

Assignment of loans

24 | What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

As a general rule, a loan claim may be assigned by an agreement between the transferor and the transferee and can be perfected by notice to or acknowledgement by the borrower with an instrument bearing a fixed date stamp.

However, it is less likely that the loan claims are assigned or perfected in a peer-to-peer or marketplace lending platform.

Securitisation risk retention requirements

25 | Are securitisation transactions subject to risk retention requirements?

Financial institutions subject to the Basel Capital Accord in Japan are subject to risk retention requirements in respect of their securitisation exposures, while the originators or sponsors are not directly subject to the same requirements. The financial institution is required to apply an increased regulatory capital risk weighting (namely, three times

higher than that otherwise applied to the compliant securitisation exposure, up to 1,250 per cent) to its securitisation exposure unless it can confirm that:

- the originator retains at least 5 per cent of the aggregate credit risk of the relevant securitised assets in any of the prescribed ways; or
- the relevant securitised assets are not inappropriately originated based on the originator's involvement in or the quality of the relevant assets, or any other circumstances.

However, it is less likely that the risk retention requirements should be considered in a peer-to-peer or marketplace lending platform.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

While it is less likely that a special purpose company is used to purchase and securitise peer-to-peer or marketplace loans, a lending platform operator extending loans to the borrowing participants must comply with the Personal Information Protection Act, which is one of the primary data protection laws in Japan.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 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.

Distributed ledger technology

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

No.

Cryptoassets

29 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 crypto-backed stabelcoins, may be regulated as a crypto-asset 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).

Such a service provider may be alternatively regulated as an electronic payment instruments (namely, fiat-backed stablecoins) service provider under the amended PSA which will become effective within one year after 10 June 2022. 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 crypto-asset 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 Payment Services Act.

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 or the Payment Services Act.

An electronic payment instruments service provider, which will be introduced by the amended PSA, which will become effective within one year after 10 June 2022, 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

30 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 which are regarded as securities is regulated under the Financial Instruments and Exchange Act (FIEA), while an ICO that deals with tokens which 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.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 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

32 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

33 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

34 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

35 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

36 | 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

37 | 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

38 | 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

39 | 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, item 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

40 | 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, Copyright Act, Trademark Act and 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

41 | 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

42 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; or
  - 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

43 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

44 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 grant of a five-year period of stay.

ANDERSON MŌRI & TOMOTSUNE

Ken Kawai
ken.kawai@amt-law.com

Akihito Miyake
akihito.miyake@amt-law.com

Tomoyuki Tanaka
tomoyuki.tanaka@amt-law.com

Yutaka Shimoo
yutaka.shimoo@amt-law.com

Kensuke Inoue
kensuke.inoue@amt-law.com

Otemachi Park Building
1-1-1 Otemachi, Chiyoda-ku
Tokyo 100-8136
Japan
Tel: +81 3 6775 1000
www.amt-law.com

UPDATE AND TRENDS

Current developments

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

It has been reported that the Bank of Japan (BOJ) has no plans to issue any central bank digital currency (CBDC). To ensure the stability and efficiency of the entire payment and settlement system, however, the BOJ has highlighted the importance of being well prepared to respond to changes. In line with this, in April 2021, the BOJ began exploring the technical feasibility of a general-use type of CBDC. In parallel with this, the BOJ also plans to study the institutional design aspects of CBDCs.

Web3 business and Metaverse-related business is gaining ground. On 7 June 2022, the Cabinet approved the Basic Policy on Economic and Fiscal Management and Reform 2022 for a New Form of Capitalism, which includes the promotion of Web3, non-fungible token and digital space business.

Luxembourg

Cathrine Foldberg Møller, Julie Carbiener, Camille Saettel, Nessym Tir and Camille Bénézet

Simmons & Simmons

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. 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 providers are already active in the country.

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 at the workplace. The local regulator, 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 intents 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 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.

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.

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 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 Insurance Commissioner.

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 the EU Directive 2015/2366 on payment services (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 for 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;
- 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;
- issuance of electronic money; and
- investment services in the sense of MiFID II (Directive 2014/65/EU), 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 (ie, a firm or a credit institution with its head office outside of the EU) can under certain circumstances provide investment services or activities to professional clients or eligible counterparties (as defined in MiFID II (Directive 2014/65/EU)) 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: Canada, Switzerland, USA, Japan, Hong Kong, Singapore, UK, China and Australia.

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 Luxembourg 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 (1) to a limited circle of previously determined persons or (2) the nominal value of a loan amounts 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);
- 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 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 AIFMD (Directive 2011/61/EU) and the implementing Luxembourg law of 12 July 2013 on alternative investment fund managers. 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?

AIFMs 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.

The EU Regulation on European crowdfunding service providers for business ((EU) 2020/1503) 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 consumer 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.

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 (Directive 2015/2366). 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 PSDII 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;
- 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;
- issuing of payment instruments and/or acquiring of payment transactions;
- money remittance;
- payment initiation services (ie, 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 (ie, 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 AISP website. Like in the rest of the EU, the drive for open banking was driven by PSDII 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 Luxembourg Insurance Sector Regulator (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, the PRIIPs Regulation (Regulation (EU) No. 1286/2014) 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, EU Regulation No. 1060/2009 on credit rating agencies applies. Under this Regulation, a credit rating agency has to be registered if it is established in a member state.

Agencies have to adopt measures to prevent conflicts of interest and ensure that its credit ratings are based on 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 a member state under one of the EU Single Markets Directives may be able to benefit

from the European Passport 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 the European Passport 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, the Markets in Financial Instruments Directive 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 a European passport or on a cross-border basis from a third country provided that certain criteria are respected and depending on the type of clients.

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 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, the Markets in Financial Instruments Directive, 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.

CHANGE OF CONTROL

Notification and consent

20 | 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 regulator and is subject to approval by the regulator.

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

21 | 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 (FATF) guidelines for 'virtual asset service providers' to register with the Luxembourg Financial Sector Regulator (CSSF) for Anti Money Laundering/ Combatting Financing Terrorism (AML/CFT) 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 MiFID II) and electronic money (as defined by the Payment Services Directive.

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

22 | 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 the 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.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

For a loan agreement to be enforceable the normal conditions applicable to contracts apply (capacity, consent and a defined and lawful subject matter). Enforceability of security agreements depends on the underlying asset. Generally, they will need to be in writing and in certain instances require a notarial deed. To ensure the enforceability it will be necessary to ensure the perfection of the security arrangement. For contracts entered into on a platform, the provisions of the Consumer Code will be applicable when a consumer is involved.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

To perfect an assignment of loans governed by Luxembourg law, notification to the debtor is required. The consent of the debtor is not required. If the assignment is not duly perfected the debtor can continue to pay the initial creditor and validly discharge its payment obligations and the assignee will not be able to enforce its rights. It is possible to contractually assign the loans without informing the borrower; however, such assignment will not be enforceable until this is completed.

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

The risk retention rules as set out in the EU Securitisation Regulation (Regulation (EU) 2017/2402) apply to P2P securitisations that are offered to European banks, investment firms, alternative investment funds or insurers. Under these risk retention rules, certain investors (such as credit institutions, Markets in Financial Instruments Directive-regulated firms and AIFMs) are subject to higher regulatory capital charges when they invest in securitisation positions that do not comply with the risk retention rules. Those rules require that either the sponsor, originator or original lender in respect of the securitisation explicitly discloses to the investor that it will retain, on an ongoing basis, a material net economic interest in the securitisation (which in any event is not less than 5 per cent) using one of five prescribed retention methods. Those methods include (among others) retention of:

- the most subordinated tranche or tranches, so that the retention equals no less than 5 per cent of the nominal value of the securitised exposures;
- 5 per cent of the nominal value of each of the tranches sold to investors; or
- randomly selected exposures equivalent to no less than 5 per cent of the nominal value of the securitised exposures.

Definitions of 'sponsor', 'originator' and 'original lender' are set out in the EU Securitisation Regulation. Furthermore, there is a direct requirement on the sponsor, originator and original lender to agree on an entity that will act as retention holder and to ensure compliance with the retention requirement. In the absence of agreement as to who will be the retention holder, the originator shall be the retention holder.

The EU Securitisation Regulation does not explicitly set out the jurisdictional scope of the 'direct' retention obligation, but there is a helpful note in the Explanatory Memorandum to the European Commission's original proposal for the EU Securitisation Regulation that the intention is that the 'direct' approach does not apply to securitisations (including P2P securitisations) where none of the originator, sponsor or original lender is 'established in the EU'. The European Banking Authority has stated that the 'direct' obligation applies only to originators, sponsors and original lenders established in the EU as suggested by the Commission in the explanatory memorandum.

'Establishment' is typically described by reference to the jurisdiction in which the legal entity is incorporated or has its registered office. Therefore, the non-EU subsidiary of an EU entity may not be subject to the 'direct' retention obligation because a subsidiary is typically a separate legal entity, whereas a non-EU branch of an EU entity may be caught within this provision because of securitisation confidentiality and data protection requirements.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

Yes, a special purpose vehicle that is based in Luxembourg will fall under the scope of these laws if it processes personal data in relation to activities in Luxembourg.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 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. 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 the 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.

Distributed ledger technology

28 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 DLT, for dematerialised securities.

In January 2022, the CSSF published a white paper on Distributed Ledger Technology 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

29 | 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 specific regulatory framework in place covering crypto-assets. 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 crypto-assets, 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 AML angle.

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

30 | 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. Generally, most tokens are by their design outside the scope of the CSSF's supervision, although this is likely to change in the future. Tokens can in certain instances be qualified as securities and would therefore be subject to regulation.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 | 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 the General Data Protection Regulation (GDPR) (Regulation EU 2016/679). 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.

As a 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, 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.

Cybersecurity

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

Luxembourg implemented Directive EU 2016/1148 (NIS Directive) by way of the law of 28 May 2019, establishing a framework for the security of network and information systems of general interest for public security. This law applies to 'vital' providers in the sectors of banking and financial market infrastructures. The CSSF is the competent authority for compliance and enforcement in the financial sector.

The Payment Services Directive (EU) 2015/2366 (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 the Payments Services Directive by way of the law of 20 July 2018.

Finally, the expected regulation on Digital Operational Resilience for the EU financial services sector will create a regulatory framework streamlining IT security in the financial sector.

Furthermore, the GDPR includes a few provisions relating to the security of the processing of personal data.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

33 | 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 EBA 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 of the financial sector (PFS) 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 interests, 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

34 | 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

35 | 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

36 | 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. This means that 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

37 | 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 (1) the exploitation is separate from the other joint owners' exploitation, and (2) this individual exploitation will not harm the work (article 5 of the law of 18 April 2001).

Trade secrets

38 | 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 (EU) 2016/943). 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.

During court proceedings, trade secrets are protected under the conditions set out in article 14 of the law of 26 June 2019, stating that protection may be granted by the judge on the request of a disputing party.

Branding

39 | 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, Luxembourg and the Netherlands) or by EU trademark (covering the 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

40 | 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

41 | 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.

TAX

Incentives

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

Luxembourg has not introduced 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 this sector.

Luxembourg benefits from one of the lowest VAT rates within the EU (ie, 17 per cent) and a moderated corporate income tax rate (ie, the overall rate of 24.94 per cent including municipal business tax and solidarity surcharge). One of the huge strengths of the country is its extended network of double tax treaties, which guarantees the absence 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 R&D activities can benefit from financial support in addition to the specific IP regime.

On top of these advantages, incorporation 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 talent. With the specific tax regime applicable to patriates, foreign talents coming to Luxembourg may benefit, subject to certain conditions, from a tax exemption for certain costs borne by their employer and of certain benefits granted by the latter in the context of the relocation of the employee to Luxembourg.

Increased tax burden

43 | 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 regulation of the fintech sector. For instance, there are no specific tax laws regulating cryptocurrencies or crypto-assets. The only relevant regulation is the administrative circular issued by Luxembourg tax authorities in 2018, where they stated in summary that cryptocurrencies are not to be considered as functional currencies for tax purposes and that the taxpayer should qualify a crypto-asset according to general tax principles and apply the related tax treatment to the income derived from said asset.

However, the fintech sector has significantly evolved since 2018.

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 the Directive on Administrative Cooperation (so-called DAC 8), it is expected that reporting obligations and subsequent obligations of exchange of information would be imposed on crypto-asset service providers and issuers. DAC 8 is still at the very beginning of the EU legislative process but there is no doubt that this new set of obligations will go ahead and become a reality for all concerned EU taxpayers.

IMMIGRATION

Sector-specific schemes

44 | 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.

simmons+simmons

Cathrine Foldberg Møller
cathrine.foldberg-moller@simmons-simmons.com

Julie Carbiener
julie.carbiener@simmons-simmons.com

Camille Saettel
camille.saettel@simmons-simmons.com

Nessym Tir
nessym.tir@simmons-simmons.com

Camille Bénézet
camille.benezet@simmons-simmons.com

Royal Monterey
26A Boulevard Royal
Luxembourg
L-2449
Luxembourg
Tel: +352 26 21 16 01
Fax: +352 26 21 16 02
www.simmons-simmons.com

UPDATE AND TRENDS

Current developments

45 | 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 proposal for the Markets in Crypto-assets Regulation at European level will be a game-changer for the fintech space. With the current proposed text, we see welcome harmonisation of the requirements across the European Union and authorised service providers will be able to benefit from the European passport to provide regulated services on a cross-border basis, as we know for many other regulated financial services. Although the text is in the process of finalisation, this will have a big impact on the legislation and regulatory requirements for fintech institutions in the near future.

Malta

Leonard Bonello and James Debono

Ganado Advocates

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 technology revolution by setting up the dedicated FinTech and Innovation function. The MFSA 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 programme interfaces in financial services;
- fostering international links to enhance bilateral cooperation and cross-border fintech knowledge, adoption and investment;
- cultivating knowledge by the 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 (2014/65/EU) (MiFID II) 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) (PSD 2) 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 provision 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.

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 in 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.

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 the MiFID II 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 the 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 marketplaces 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.

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 PSD 2. 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 the 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.

CHANGE OF CONTROL

Notification and consent

20 | 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

21 | 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.

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

22 | 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.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Loan and security agreements are contracts that are generally governed by Maltese contract law. In this respect, the parties entering into such an agreement must have the capacity to do so, which, in the case of companies, means that the agreement is signed by a director after having obtained proper authorisation from the board. In the case of natural persons, contracts can generally be entered into by anyone over the age of 18, provided that they have not previously been interdicted or incapacitated. Depending on the type of loan or security agreement that is being entered into, special laws may apply. In the context of a pledge of shares, special rules contained in the Companies Act, Chapter 386 of the Laws of Malta, will also apply, which requires the pledge to be constituted by an instrument in writing and notified to the Malta Business Registry.

Given that loan and security agreements are determined by contract between the parties, enforcement depends on the provisions of the respective contracts; however, parties are not precluded from enforcing an agreement before the Maltese courts or by instituting arbitration proceedings in Malta.

Assignment of loans

24 | What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

The assignment of loans and other rights is generally dealt with in the Civil Code, Chapter 16 of the laws of Malta. The Civil Code provides that an assignment is complete and the ownership of the thing being assigned is acquired by the assignee as soon as the thing is transferred, the price has been agreed and when the deed of assignment (which must be in writing) is made. The assignee may not exercise the rights assigned to them, except against third parties after due notice of the assignment (by judicial act) has been given to the debtor; however, notice is not necessary if the debtor has acknowledged the assignment.

However, Malta's securitisation framework, based on the Securitisation Act, Chapter 484 of the Laws of Malta, operates as an opt-in regime whereby legal entities entering into securitisation transactions may style themselves as securitisation vehicles subject to the Securitisation Act, which aims to facilitate securitisation transactions by, among other things, relaxing some of the requirements regarding the assignment of rights as set out in the Civil Code. An assignment of rights (to a securitisation vehicle) made pursuant to the Securitisation Act:

- does not require the assignment to have a price;
- is complete as soon as the assignment is written; and
- allows notice to be given to debtors by a simple written notice (namely, not a judicial act) or by publication of a notice in a daily newspaper.

An assignment made properly under the Securitisation Act is considered a true sale as the Securitisation Act provides that such an assignment will be treated as final, absolute and binding on the assignor (the originator), the assignee (securitisation vehicle) and all third parties and is not subject to clawback. This implies that an assignment that is not perfected under the Securitisation Act may not be considered a true sale and may be subject to annulment, rescission, revocation or termination.

Securitisation risk retention requirements

25 | Are securitisation transactions subject to risk retention requirements?

The Securitisation Regulation (Regulation (EU) 2017/2402) became directly applicable to all EU member states from 1 January 2019. Article 6 of the Securitisation Regulation directly tackles risk retention, providing that, subject to any exceptions set out therein, the originator, sponsor or original lender of a securitisation must retain, on an ongoing basis, a material net economic interest in the securitisation of no less than 5 per cent. In the circumstance that the retainer of this risk was not agreed, the originator must by law retain the risk.

Securitisation confidentiality and data protection requirements

26 | Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

The Securitisation Act provides that the transfer of any data or information made in the context of a securitisation transaction must remain subject to professional secrecy, confidentiality and data protection laws. However, transfers of personal data made in the context of a securitisation are carried out to give effect to a contract or are otherwise deemed to have been made for the legitimate interest of the transferee and transferor unless it is shown that this interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject. Transfers of personal data made to a third country that does not ensure an adequate level of protection within the meaning of the General Data Protection Regulation (Regulation (EU) 2016/679) are required to be carried out subject to additional safeguards, including standard contractual clauses or binding corporate rules.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 | 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.

Distributed ledger technology

28 | 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

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

Cryptoassets 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.

Token issuance

30 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.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 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 the 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

32 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

33 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

34 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

35 | 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

36 | 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

37 | 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

38 | 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

39 | 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

40 | 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

41 | 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 anti-competitive 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

42 | 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

43 | 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.

ganado advocates

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.ganado.com

IMMIGRATION

Sector-specific schemes

44 | 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

45 | 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.

Netherlands

Koen van Leeuwen, Jeroen Bos, Meike Hoekstra and Marise Kok

Simmons & Simmons

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 PSD2). Generally, diversification in the Dutch financial services sector is increasing as new entrants enter the market and incumbents (such as large Dutch banks) progress their own fintech initiatives.

In addition, despite the additional administrative and compliance costs of the Dutch registration regime for certain crypto service providers that has applied since May 2021, many large (and smaller) crypto service providers seem keen to enter and provide their services to the Dutch 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?

In 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. Within the InnovationHub, the AFM and DNB cooperate with the Dutch Authority for Consumers and Markets (ACM). The InnovationHub aims to offer easy access to supervisors and regulators for companies that provide innovative services or products, remove any unnecessary barriers to entry, gain more insight into the rapidly developing technological innovation within the financial sector, and improve knowledge, sharing and dialogue with all relevant stakeholders. The InnovationHub enables fintech companies to obtain a temporary banking licence, among other things.

The AFM and DNB have also 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.

DNB also periodically organises the seminar 'Fintech meets the Regulator', during which relevant market participants and DNB share thoughts on current developments.

Additionally, in November 2019, DNB launched the iForum, a platform for joint initiatives intending to create value for the Dutch sector and DNB. Via the iForum, the Dutch sector and DNB can have a dialogue on the impact of technological innovations on the sector and develop joint pilots and experiments.

Furthermore, in April 2020, DNB stated that it has a favourable attitude towards central bank digital currency (CBDC). CBDC is money issued by a central bank and generally accessible to households and business. Therefore, DNB does not only support financial innovation, but also intends to play a leading role in certain financial innovation, such as the development of CBDC.

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 on the online use of personal data by algorithms, among other things, and will coordinate how to enforce (new) European 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 DNB maintain contact with other regulators in the Netherlands (such as the ACM, the AP and the CvdM), the EU 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 DNB supervise compliance with 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 the Revised 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.
- 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.
- Clearing and settlement: acting as a clearing and settlement institution requires a licence.
- 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 and 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 the Alternative Investment Fund Managers Directive (AIFMD), or an undertaking for collective investment in transferable securities, as defined in the Undertakings for Collective Investment in Transferable Securities Directive (UCITSD).

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 (1) facilitate granting of loans (excluding consumer credit) (loan-based crowdfunding); or (2) 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 MiFID II 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. After this date, they require a licence from the AFM under the EU Crowdfunding Regulation. Only existing CSPs that submitted a licence application with the AFM by 10 May 2022 at the latest can avail themselves of this transitional regime.

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 on the basis of 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;
- 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;
- 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 doubt;
  - 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 II and suitability guidelines published by the European Securities and Markets Authority (ESMA) 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 and was submitted to Parliament in November 2021.

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 (the Capital Requirements Directive, Solvency II, the Markets in Financial Instruments Directive II, the Insurance Distribution Directive, the Mortgage Credit Directive, the Undertakings for Collective Investment in Transferable Securities Directive, the Alternative Investment Fund Managers Directive and the Revised Payment Services Directive) may, in principle, provide cross-border services into or establish a branch in the Netherlands.

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 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.

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 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 Dutch Financial Supervision Act.

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 Further Regulation on Conduct of Business Supervision of Financial Undertakings (the Further Regulation).

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 (ie, the name of the provider, the regulatory status of 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.

Furthermore, the Dutch Authority for the Financial Markets 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).

CHANGE OF CONTROL

Notification and consent

20 | 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 UCITS, 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 of qualifying holdings above certain thresholds are also notifiable to or subject to approval from DNB.

This also applies to any qualifying holdings in Dutch registered crypto service providers.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

21 | 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. However, as of 21 May 2020, certain crypto service providers fall with 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 (ie, 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 Dutch language, etc). Non-EEA crypto service providers are currently not eligible for registration.

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 Sanctions Act, transaction monitoring, reporting of unusual transactions to the Financial Intelligence Unit-Netherlands and customer due diligence must be covered. Furthermore, DNB applies a 'wallet verification requirement' in relation to incoming and outgoing transactions.

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

22 | 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 (AFM) and DNB have set up the InnovationHub to support market operators, such as fintech companies. Furthermore, DNB has published a brochure entitled 'Good practices fighting corruption' and the DNB website provides answers to questions regarding DNB's integrity supervision of crypto service providers. As regards anti-money laundering and combating financing of terrorism, DNB issued a comprehensive guidance in December 2020 titled 'Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act' which also relates to trade sanctions.

In addition to the InnovationHub, the 'Regulatory Sandbox' was launched in 2017 by DNB and the AFM. While the InnovationHub is meant to facilitate fintech start-ups with qualifying their contemplated business model and assessing the applicability of financial regulatory laws on such business model, the Regulatory Sandbox is supposed to go a step further. The Regulatory Sandbox was created to further facilitate innovation and to enable enterprises to launch their innovative financial products without any hinderance. The Regulatory Sandbox enables fintech companies to discuss a customised approach if they experience disproportionate regulatory obstacles. In the Regulatory Sandbox, applicants can seek the assessment of the relevant regulator to assess whether innovative concepts comply with the underlying purposes of the applicable financial market regulations rather than the letter of the law, hereby creating a dialogue between a business and its applicable regulator.

After the success of the Regulatory Sandbox, DNB created an innovation forum with the name iForum. The iForum can be categorised as a hub for joint initiatives that create value for both DNB and supervised institutions, such as banks, insurers and pension funds.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Loan agreements are not restricted to a certain form and can therefore be entered into and executed electronically. To create a security right (ie, a right of pledge or mortgage) a deed is required, which has to be in writing. Dutch law distinguishes between authentic deeds, which require the involvement of a civil law notary (and can therefore not be executed in electronic form), and private deeds (which will need to be disclosed to the relevant parties or be registered with the Dutch Tax Authority).

A private deed can be executed electronically provided its contents are stored for future reference during a minimum relevant period (depending on the nature of the deed) in such a way that they can be reproduced without alteration. For example, a deed of pledge can be executed electronically provided that the pledgee can store the deed during the duration of the loan agreement for which the pledge was issued. In addition, the deed still needs to be printed as the Dutch Tax Authority does not accept electronic copies of a deed.

An electronic deed will require an electronic signature. An electronic signature can constitute proof of the intention of the signatory to agree with the contents of a certain document in the same way a written signature does if the method used to authenticate the electronic signature is sufficiently reliable. The Dutch courts asses the reliability of this method in view of all the circumstances of the relevant case.

There is no specific risk that loan agreements or security agreements will not be enforceable when entered into on a P2P or marketplace lending platform.

Assignment of loans

24 | What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

Under Dutch law, there is a distinction between the transfer of loans (ie, the receivables and the liabilities under a loan) and the sole assignment of receivables under the loans. As securitisations require that only the receivable is assigned, only the assignment of receivables is discussed here.

Assignment always requires that: (1) the receivable is transferable; (2) the seller holds legal title to the receivable; (3) there is a valid title for the assignment (an agreement usually); and (4) the receivable is delivered. Delivery can be perfected by way of an undisclosed assignment or disclosed assignment.

An undisclosed assignment requires an executed deed, either in notarial form or in private form, to be registered with the Dutch Tax Authority. Perfection takes place the moment the deed is executed by the notary or at the time of registration with the Dutch Tax Authority. Receivables may only be transferred by way of undisclosed assignment if they: (1) exist at the date of registration or execution of the deed of assignment; or (2) are future receivables directly resulting from a legal relationship existing at the date of assignment.

A disclosed assignment requires that notification of the assignment is given to the debtor.

If the (delivery of the) assignment is not perfected, the receivable has not been successfully assigned to the assignee. If the seller

becomes insolvent before all conditions for the assignment have been perfected, the receivables can no longer be assigned and the insolvent seller remains the owner.

Until notification of the assignment, borrowers can only validly pay to the assignor in order to validly discharge their payment obligations, and payments made prior to notification of the assignment but after the assignor has been declared insolvent will fall in the estate of the assignor.

Assignment of receivables does not require the consent of the borrower or informing the borrower. Assignment of receivables only requires notification to the borrower in the case of a disclosed assignment. A contractual non-assignment clause may prevent the transfer of receivables, depending on the exact wording of the clause.

Securitisation risk retention requirements

25 | Are securitisation transactions subject to risk retention requirements?

The risk retention rules as set out in the EU Securitisation Regulation apply to P2P securitisations that are offered to European banks, investment firms, alternative investment funds or insurers. Under these risk retention rules, certain investors (such as credit institutions, Markets in Financial Instruments Directive-regulated firms and alternative investment fund managers) are subject to higher regulatory capital charges where they invest in securitisation positions that do not comply with the risk retention rules. Those rules require that either the sponsor, originator or original lender in respect of the securitisation explicitly discloses to the investor that it will retain, on an ongoing basis, a material net economic interest in the securitisation (which in any event is not less than 5 per cent) using one of five prescribed retention methods. Those methods include (among others) retention of:

- the most subordinated tranche or tranches, so that the retention equals no less than 5 per cent of the nominal value of the securitised exposures;
- 5 per cent of the nominal value of each of the tranches sold to investors; or
- randomly selected exposures equivalent to no less than 5 per cent of the nominal value of the securitised exposures.

Definitions of 'sponsor', 'originator' and 'original lender' are set out in the EU Securitisation Regulation. Furthermore, there is a direct requirement on the sponsor, originator and original lender to agree on an entity that will act as retention holder and to ensure compliance with the retention requirement. In the absence of agreement as to who will be the retention holder, the originator shall be the retention holder.

The EU Securitisation Regulation does not explicitly set out the jurisdictional scope of the 'direct' retention obligation, but there is a helpful note in the Explanatory Memorandum to the European Commission's original proposal for the EU Securitisation Regulation that the intention is that the 'direct' approach does not apply to securitisations (including P2P securitisations) where none of the originator, sponsor or original lender is 'established in the EU'. The European Banking Authority (EBA) has stated that the 'direct' obligation applies only to originators, sponsors and original lenders established in the EU as suggested by the Commission in the explanatory memorandum.

'Establishment' is typically described by reference to the jurisdiction in which the legal entity is incorporated or has its registered office. Therefore, the non-EU subsidiary of an EU entity may not be subject to the 'direct' retention obligation because a subsidiary is typically a separate legal entity, whereas a non-EU branch of an EU entity may be caught within this provision because a branch is typically not a separate legal entity. Market participants are still seeking clarity on this and it is expected that this point will be raised as part of the ongoing EBA consultation on risk retention.

Securitisation confidentiality and data protection requirements

26 | Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

Yes, a special purpose vehicle that is based in the Netherlands will fall under the scope of these laws if it processes personal data in relation to activities in the Netherlands.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 | 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). However, on 21 April 2021, the European Commission published a draft Regulation on the use of AI. The purpose of this Regulation is to lay down rules for the development, marketing and use of AI.

Furthermore, at the moment there is no specific regulation on automated investment advice. However, the Dutch Authority for the Financial Markets (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, MiFID II and suitability guidelines published by the European Securities and Markets Authority (ESMA) 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, Dutch draft legislation on automated advice was published as part of a publication consultation. This legislation aims to introduce safeguards in order 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 and was submitted to Parliament in November 2021.

Distributed ledger technology

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

Other than the General Data Protection Regulation, currently no specific rules or regulations apply that govern the use of distributed ledger technology (DLT) or blockchain. The use of DLT is subject to the existing regulatory legislation depending on its application in any particular case. DLT is a subject that has led to many questions in the InnovationHub.

However, as of 23 March 2023, the EU Regulation on a pilot regime for infrastructures based on DLT will apply. This Regulation aims to lay down requirements on multilateral trading facilities and securities settlement systems using DLT.

Cryptoassets

29 | 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 Dutch Financial Supervision Act (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.

Furthermore, 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 services provided by electronic money institutions. In these circumstances, unless an exemption applies, the relevant activities trigger a licence requirement 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 DNB.

On 24 September 2020, the European Commission published a draft Markets on Cryptoassets (MiCa) Regulation. Under the MiCa Regulation, currently out-of-scope assets and service providers will be regulated. Under this MiCa Regulation, cryptoassets are categorised as utility tokens, asset-referenced tokens or e-money tokens. This categorisation also covers stablecoins.

Cryptoassets that are currently regulated (for example as financial instrument or e-money) will not fall within scope of the MiCa Regulation.

Furthermore, the MiCA Regulation will regulate certain crypto-asset services, including:

- custody services;
- the operation of a crypto trading platform;
- the operation of a crypto exchange;
- crypto-to-crypto transactions;
- the execution of client orders in cryptoassets;
- placing of cryptoassets;
- the transfer of cryptoassets;
- the receipt and transmission of client orders in cryptoassets;
- providing advice on cryptoassets;
- the exchange of cryptoassets for financial instruments; and
- the provision of portfolio management on cryptoassets

Among other things, the MiCa Regulation introduces a licensing regime for crypto asset service providers (CASPs) and issuers of cryptoassets. Furthermore, issuers of cryptoassets will be required to publish a White Paper setting out the core information on these cryptoassets.

In March 2022, the European Parliament published the latest draft of the MiCA Regulation. It is the expectation that the MiCa Regulation will enter into force not later than by 2024.

Token issuance

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

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 scope of the FSA on the basis of activities provided in relation to these currencies.

Furthermore, crypto service providers that provide exchange services between virtual and fiat currency (for example by operating a crypto exchange) in or from the Netherlands are required to register with DNB. Additionally, digital currency exchanges, crypto-brokers and issuers may fall within scope of the future MiCa Regulation.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 | 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 General Data Protection Regulation (GDPR) came into force with direct effect across the entire EU. 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 – 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 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. Other lawful bases for processing data (and commonly used in case of the processing of employee 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 the legal obligations of the business.

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.

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. However, for the data to have been effectively anonymised, the data subject must no longer be identifiable – which is a question of how far businesses have to go to ensure true anonymisation.

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.

There are no legal requirements or regulatory guidance relating to personal data that are specifically aimed at fintech companies.

Cybersecurity

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

The Revised 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 on 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.

Secondly, payment service providers must notify DNB as to any grave 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. Last but not least, the payment service provider must inform users of the measures taken to mitigate 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 (NCSC). 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).

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.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

33 | 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. Furthermore, 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 required activities under the Dutch Money Laundering and Terrorist Financing (Prevention) Act) further detailed outsourcing provisions apply.

Cloud computing

34 | 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. 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. 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. Furthermore, the financial institution is required to have adequate policies and proper procedures to manage outsourcing risks.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

35 | 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.

Programs for computers 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 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

36 | 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

37 | 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.

Trade secrets

38 | 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 the EU Trade Secrets Directive (Directive 2016/943/EU). The Trade Secrets Act provides more specific rules for the protection for 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 good, which are goods, the design, characteristics, functioning, production process or marketing of which significantly benefits 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 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

39 | 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 EU (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

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

Remedies 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 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

41 | 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 in all sectors and including therefore also the financial sector. By means of the Financial Sector Monitor (FSM), 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. Furthermore, 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 which 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 in respect of front-end providers 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 PSD2 and the European Commission's Regulatory Technical Standards (RTS), 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 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 (Apple, Amazon, Ant Group, 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 in order to reinforce their ecosystems, rather than being driven by the introduction of PSD2.

The ACM identified the following competition risks:

- access restrictions for new innovative players such as Big Tech and fintechs; and
- Big Tech leveraging their dominant market position in neighbouring markets to tip the payment market (through self-preferencing).

The ACM concluded that an amendment of PSD2 may be in order to ensure that it also applies to Big Tech that are 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 proposed Digital Markets Act, which, once adopted, will create 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 mandate the app provider to use Apple's payment system for the processing of payments and stipulate that app providers are not allowed to refer within their own apps to payments options outside the app, for example to alternative payments options that app providers offer on their websites. According to the ACM, this constituted an abuse of a dominant position.

TAX

Incentives

42 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. However, there are certain tax incentives available to 'innovative' companies. The key incentives are:

- WBSO (R&D payroll tax credit) – allows an employer a payroll tax refund of 16 per cent to 32 per cent of the salary costs that an employer has paid to its employees who conduct R&D activities;
- innovation box – allows companies to have profits derived from qualifying IP income taxed at an effective corporate income tax rate of 9 per cent instead of the regular corporate income tax rate of 15 per cent to 25.8 per cent; and
- costs incurred in connection with the development of intangible assets may be depreciated (amortised) at an accelerated rate – instead of capitalised and depreciated over the technical or economic life span of the asset.

A number of conditions must be met in order to qualify for each tax incentive scheme. In general, directors (or employees) who also hold a substantial interest in a company (at least 5 per cent) should receive (or if not actually received, are deemed to receive) an annual salary from their company of at least €48,000 (in respect of which payroll taxes are payable) unless it can be demonstrated that others performing similar activities earn less. For a start-up company, the deemed salary may be lowered to the minimum wage in the Netherlands (€1,756.20 a month as of 1 July 2022) as a result of which less payroll taxes are payable.

On 31 May 2021, a Dutch legislative proposal was published with respect to the taxation of holders of stock options. Under the proposal, other than under the normal rule whereby income is recognised upon exercise of an option, options can still be exercised but income taxation can be deferred until the moment the stock becomes tradeable. This offers a solution to the problem that tax may be paid at a time when insufficient liquidity is available. However, at the employee's discretion, taxation can still take place at the moment of exercise of the stock options. The proposal would become effective on 1 January 2023.

Increased tax burden

43 | 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.

IMMIGRATION

Sector-specific schemes

44 | 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 (of course, 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 EU, 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 2021 that vary from €2,497 to €4,752, 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 masters or PhD (if graduation is from a university in the Netherlands then bachelor level is also allowed). These salary thresholds are indexed each year. Next to that, the formal employer in most cases needs to be recognised as a sponsor for the purpose of regular labour and knowledge migrants. If the employer is not such a recognised sponsor, the employer can apply for that or make use of a payroll company that is recognised as such a 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.
- Intra-corporate transfer scheme (Directive 2014/66/EU): if the employee is a specialist, manager or trainee and remains on the payroll of his or her employer outside the EU, and the employee was already employed at that entity outside the EU 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, for example, a residence permit as a knowledge migrant. A residence permit as an intra-corporate transferee cannot be prolonged if, with that prolongation, the maximum duration of one (trainee) or three (specialist or manager) years is exceeded). No salary thresholds are applicable, albeit that the salary needs to be in conformity 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. 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 precedent 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): the EU version of the Dutch knowledge migrant scheme but with a higher salary threshold, and where specific education requirements apply. The salary threshold in the Netherlands is €5,567 gross per month, exclusive of holiday allowance for 2021. This salary threshold is indexed each year. Recognised sponsorship is not required but is nevertheless advisable due to the more rapid application procedure. 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.
- International trade regulation: a relatively new 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 2021 increased from €1,684.80 gross per month to €1,701 gross per month, exclusive of 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 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 €3,484 to €4,752 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, 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 assemble, repair, install, amend and instructing on the use of those goods, which includes software: the name speaks for itself. 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.

- Researcher (Directive 2016/801/EU): mostly for researchers and scientists working at universities and other research institutions and companies. A specific recognised sponsorship is necessary for the purpose of educational institution. The researcher will work as either a paid researcher, an unpaid researcher with a grant or as a PhD candidate and complies with the admittance requirements. Other specific requirements are applicable. The researcher must have at least €1,179.36 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 EU. A residence permit obligation applies after 90 out of 180 days. It is specifically for third-country nationals living and working legally in EU member state A and temporarily performing services or work for their employer in member state B. No salary threshold applies and no recognised sponsorship is needed. Next to that, 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 than stated above might suit the situation better. Next to that, 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 totally 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, very specific exemptions left aside. Sanctions in the case of non-compliance are high – normally an €8,000 fine per illegal 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, up to shutting down the operations in the Netherlands 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

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

EU developments

Significant current developments relating to fintech currently seem to be driven on a European level, as a result of the European's adoption of the Digital Finance Package in September 2020.

simmons+simmons

Koen van Leeuwen
koen.vanleeuwen@simmons-simmons.com

Jeroen Bos
jeroen.bos@simmons-simmons.com

Meike Hoekstra
meike.hoekstra@simmons-simmons.com

Marise Kok
marise.kok@simmons-simmons.com

Claude Debussylaan 247
1082 MC
Amsterdam
Netherlands
Tel: +31 20 722 2500
Fax: +31 20 722 2599
www.simmons-simmons.com

Among other things, this Digital Finance Package introduces the MiCA Regulation, the Regulation on a pilot regime for infrastructures based on DLT and the Regulation on digital operational resilience for the financial sector.

Furthermore, the European Commission published a draft Regulation on the use of AI in April 2021 and its AML/CFT Reform Package in July 2021. The latter will have a significant impact on crypto service providers.

Additionally, on 13 January 2022 the final phase for the set-up of the Unified Patent Court (UPC) commenced. The UPC will offer a single, specialised patent jurisdiction for participating EU member states.

The UPC is expected to officially open its door in late 2022 or early 2023. With the UPC, patentees will also get the option for applying for Unitary Patents, which will have effect across all participating EU member states. So far 16 EU member states have ratified the necessary legislation, and 24 are expected to do so. 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.

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.

Nigeria

Ugochukwu Obi, Tare Olorogun, Omolade Afonja, Philips Adekemi and Anthony Obidike

Perchstone & Graeys

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 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 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 the 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. 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 the 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?

- The Central Bank of Nigeria (CBN);
- the Securities and Exchange Commission (SEC);
- the Corporate Affairs Commission (CAC);
- the National Insurance Commission (NIC);
- the Nigerian Communications Commission (NCC);
- the Nigerian Information Technology Development Agency;
- 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.

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 Rule). The Securities and Exchange Commission (SEC), a 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 ISA. The Rule also provides 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.

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 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, 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 SEC. Also, it should be noted that the CBN issued a notice to deposit money banks to refrain from facilitating payment transactions associated with cryptocurrency trading.

CHANGE OF CONTROL

Notification and consent

20 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.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

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

Yes. The CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations 2013 imposes an obligation on all financial institutions, including fintech companies to have policies on anti-money laundering 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.

Guidance

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

The following laws generally govern money laundering 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 Central Bank of Nigeria (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).

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Executing a loan agreement in Nigeria is akin to the requirements to execute a valid agreement. Under Nigerian laws, certain conditions for a valid agreement must be met, namely:

- offer;
- acceptance;
- intention to create legal relations;
- consideration; and
- capacity.

However, security documents transferring title in land such as mortgage must have the consent of the state governor as provided by the Land Use Act; or else it remains inchoate and unenforceable. Where security are movable assets (except for aircraft, ships, etc), the Secured Transactions in Movable Assets Act provides that such security be registered at the National Collateral Registry.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

Peer-to-peer or marketplace platform is still developing in Nigeria and there are no specific rules for peer-to-peer or marketplace lending in Nigeria or assignments of loans originating from these transactions. However, the Factoring Bill is currently being deliberated upon in the National Assembly and may provide for such assignment. In the meantime, the assignment of loans may largely be dealt with in accordance with the terms of the loan agreement; whether such agreement allows for the assignment of the loan to a third party without the consent of the borrower.

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

Yes, securitisation transactions are subject to risk retention. The nature of the transaction will determine the party that would retain the risk in a securitisation transaction. If the method adopted is an assignment, then the originator retains the risk. The originator by the securitisation structure buys the lower tranche of the note to insulate the other investors where there is a risk of default by the SPV to repay or there is a shortfall or where the SPV does not realise sufficient funds to meet up its repayment obligations to the investors.

Securitisation confidentiality and data protection requirements

26 | Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

Generally, the Nigerian Data Protection Regulations 2019 issued by the Nigerian Information Technology Development Agency regulate privacy and data protection in Nigeria. There are, however, no specific laws on the purchase of loans by SPVs subject to the confidentiality clause.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 | 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 (SEC) issued the Rules on Robo-Advisory Service in Nigeria, dated 30 August 2021 (the Rules) to regulate people who carry out robo-advisory services in Nigeria.

Distributed ledger technology

28 | 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, 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.

Cryptoassets

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

Yes. 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

30 | 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, SEC has released new Rules on Issuance, Offering Platforms and Custody of Digital Assets, 2022, which regulates the offering of digital assets including initial coin offering.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 | 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

32 | 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 CBN also released the Risk-Based Cybersecurity Frameworks and Guidelines for Deposit Money Banks and Payment Service Providers.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

33 | 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

34 | 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

35 | 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. 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

36 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 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 vest 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

37 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

38 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

39 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.

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

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

The remedies available to 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

41 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 startups within the fintech industry. One of these requirements is shareholders 'funds unimpaired by losses' required to be deposited with the CBN when applying for specific licences within the payment system industry.

TAX

Incentives

42 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. Currently, the Startup Bill 2021, which is before the National Assembly, may provide incentives for startups.

Increased tax burden

43 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

44 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 for 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

45 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. There is also the Startup Bill, Securitisation Bill and the Factoring Bill currently before the National Assembly.

Perchstone & Graeys
SOLICITORS ADVOCATES ARBITRATORS

Ugochukwu Obi
ugochukwuobi@perchstoneandgraeys.com

Tare Olorogun
tareolorogun@perchstoneandgraeys.com

Omolade Afonja
omoladeafonja@perchstoneandgraeys.com

Philips Adekemi
philipsadekemi@perchstoneandgraeys.com

Anthony Obidike

1, Perchstone & Graeys Close
Off Remi Olowude
Lekki Expressway
Lagos
Nigeria
Tel: +234 1 342 9131
www.perchstoneandgraeys.com

Singapore

Yingyu Wang and Ashleigh Low
Simmons & Simmons

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 report by FinTech Global, Singapore's fintech sector saw nearly a four-fold increase in funding in 2021 driven by large deals. While the overall capital invested is on track to remain stable, the spike in deal activity in the first quarter of 2022 indicates that 2022 will surpass 2021's levels to hit a total of 260 deals (compared to 207 deals in 2021).

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 June 2022, MAS had signed 36 fintech cooperation agreements with other countries, including Abu Dhabi, Australia, China, Canada, France and the United Kingdom, 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: (1) expansion of eligibility criteria to include early adopters of technology innovation, (2) streamlined application with financial grant for first movers of technology innovation, and (3) participation in Deal Fridays programme, a platform for deal-making opportunities. Sandbox Plus has been effective since 1 January 2022.

MAS has encouraged engagement with the industry and has been open to discuss 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 (APIs) 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. The FSTI 2.0 scheme is valid until March 2023.

Under FSTI 2.0, MAS will commit S$42 million towards the Regulatory Technology (RegTech) grant scheme and enhancement of 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 launched in April 2020 to help smaller FIs and FinTech firms adopt digital solutions to better cope with the impact of covid-19. In response to the 1,100 applications for the DAG scheme, MAS will commit an additional S$30 million to the DAG scheme.

MAS, the 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 fintechs manage their cash flow better, support them in generating new businesses, and provide greater support for fintechs to pursue growth strategies.

Additionally, MAS has partnered with the 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.

The following activities are regulated under the FAA:

1 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;
2 advising others by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product; and
3 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.

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 Moneylenders Act 2008 (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 activity 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.

Furthermore, 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 the MAS's FAQ on Lending-Based Crowdfunding (issued 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 entities) below S$5 million per 12-month period;
- a private placement to 50 or fewer investors within a 12-month period; or
- an offer made only to institutional or accredited investors.

These are not 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, certain payment services are now regulated in Singapore under, inter alia, the PS Act. These regulated payment service activities are:

- 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 licence: money-changing, standard payment institution or major payment institution.

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 different quantums 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 digital payment token services has been significantly increased to address Singapore's commitment to the Financial Action Task Force (FATF) 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 ATM 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-advisors 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 the 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.

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 the 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 the 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.

CHANGE OF CONTROL

Notification and consent

20 | 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

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

Under the Payment Services Act 2019 (the PS Act), digital payment token (DPT) 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 PS Act.

Such AML/CFT requirements oblige licensees to take appropriate steps to identify, assess and understand their 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

22 | 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.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Contract law in Singapore broadly follows its common law heritage, and therefore the usual elements necessary for the legality, validity and enforceability of an agreement would apply.

Therefore, provided that any peer-to-peer (P2P) or marketplace lending model complies with the requisite regulatory requirements, there should be no specific issues that affect the enforceability of an agreement just by virtue of such agreement being entered into on a P2P or marketplace lending platform (ie, the usual rules apply).

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

A legal assignment of the rights of the lender of a loan under a P2P or marketplace lending platform, under which the purchaser of that loan would be entitled to directly sue the borrower for repayment of the debt under the loan, requires notice of this assignment to be given by the assigning lender to the borrower under the loan agreement.

The ability to transfer rights and obligations in a loan under Singapore law (whether in respect of a P2P or marketplace lending platform or otherwise) will depend on the terms of the loan.

In the absence of any specific provisions regarding transfer of both rights and obligations of a borrower's position in the loan agreement, the borrower's consent would be required to transfer the borrower's rights and obligations under a loan (although, in the absence of any express provisions to the contrary, an assignment of a lender's rights only (and not the borrower's rights) would not require the giving of notice to, or the receipt of consent from, the borrower although any lack of notice may affect the nature of any assignment of these rights).

It is quite common, however, for specific transfer provisions to be included in loan agreements to allow a lender to transfer its rights and obligations in their position in a loan to a third party without any further borrower consent. Customarily, criteria will be specified as to what constitutes an eligible transferee. In certain cases, it may be necessary to notify the borrower of the transfer in order for the transfer to take effect even in circumstances where borrower consent was not required.

Any transfer would also need to comply with any related restrictions imposed under the terms of the loan agreement and under regulations applicable to particular classes of borrower.

In connection to any assignment of a lender's rights under a loan, where notice of the assignment is not given by the assigning lender to the borrower under the loan agreement, the security assignment would, in ordinary circumstances (and subject to due execution and other formalities), be characterised as an equitable assignment. In such case, any action by the purchaser to enforce rights under the loan agreement needs to be taken by the lender on behalf of the purchaser. This may delay the taking of action and have an impact on recoveries.

Any assignment will be subject to the general provisions of the loan agreement, including, without limitation, confidentiality restrictions, restrictions on the granting of security or transfers to third parties. As such, loan agreements for P2P or marketplace lending platforms that contemplate ease of assignment or transfer must be drafted to ensure that any such restrictions are kept to a minimum or excluded to the extent possible and subject to regulatory constraints applicable to lending to specific classes of borrowers.

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

The Monetary Authority of Singapore Notice 637 (the MAS Notice) (last revised on 31 March 2020) requires a reporting bank (being a bank incorporated in Singapore) to ensure that the originator of the credit claims or receivables being securitised retains a material net economic exposure and demonstrates a financial incentive in the performance of these assets following their securitisation. As such, the reporting bank is required to ensure that this originator does retain such applicable risk in the exposures.

Pursuant to MAS Notice 637, reporting banks are also subject to maximum retention thresholds in respect of securitisation exposures to the extent that this reporting bank is looking to apply regulatory capital relief in respect of these exposures, as set out in more detail in MAS Notice 637.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

Possibly. In addition, loan agreements may contain confidentiality provisions that any purchaser, including any special purpose company, is bound by. These would need to be carefully reviewed or drafted as part of any securitisation structure.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 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. However, the Monetary Authority of Singapore (MAS) has issued various publications aimed at fostering the development of artificial intelligence innovation, as well as addressing potential issues.

For example, the 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 whether the digital adviser actually provides advice 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. Veritas outlines a framework for the responsible adoption of AI and data analytics by financial institutions. MAS will commence with the development of metrics to measure the fairness of deployment of this technology. MAS has identified credit risk scoring and customer marketing as the first two workstreams in which it would like to introduce the metric.

Distributed ledger technology

28 | 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, 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 blockchain technology would be the Payment Services Act 2019 (the PS Act), under which digital payment token service providers (such as traders and exchanges) would require a licence.

Cryptoassets

29 | 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 crypto-asset is regulated, and how it would be regulated, would depend on the nature and characteristics of such crypto-asset. For example, if a crypto-asset is a security, it would likely fall within the scope of the Securities and Futures Act 2001 (SFA); if a crypto-asset is a digital payment token, 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) digital payment tokens, and facilitating the exchange of digital payment tokens. 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 digital payment token services will be expanded to capture a few more types of regulated activities in relation to digital payment tokens. 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's 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 ATMs; 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 emphasis MAS's stance that 'the trading of cryptocurrencies is highly risky and not suitable for the general public'.

Token issuance

30 | 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 crypto-asset is regulated, and how it would be regulated, would depend on the nature and characteristics of such crypto-asset. 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 or the need to register a prospectus, or both.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 | 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 PDPA for Selected Topics.

The PDPC has recently announced new 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 will provide individuals with greater control over their personal data and enable 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 new 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 a new 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. They include the following.

Collection, use and disclosure of personal data without consent is now permitted in the event that this is in the general legitimate interests of the organisation

To rely on this broad exemption, an organisation must:

- identify the legitimate interest;
- conduct an assessment to identify any adverse effect on the individual and implement reasonable measures to reduce any such effects; and
- disclose reliance on the legitimate interests exception.

Business improvement exception

Organisations may use personal data of users without their consent where:

- improving, enhancing or developing new goods or services;
- improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;
- learning or understanding behaviour and preferences of individuals; or
- identifying goods and services that may be suitable for individuals, or personalising and customising goods and services for such individuals.

Cybersecurity

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

While there is a new cybersecurity law – the Cybersecurity Act 2018, which 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.

With regard to regulated fintech companies, the Monetary Authority of Singapore (MAS) issued a consultation in March 2019 seeking feedback to expand the Technology Risk Management Guidelines to include guidance for the following:

- technology risk governance and oversight;
- best practices for software development;
- additional guidance for new technologies (ie, 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.

In September 2018, MAS also sought to strengthen the rules on cybersecurity 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 cybersecurity 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.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

33 | 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.

The 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

34 | 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 the 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

35 | 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

36 | 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

37 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

38 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

39 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

40 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

41 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

42 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 deduction 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 (S13H) 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 bonus received from an approved venture capital fund. To benefit from both S13H and 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

43 | 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

44 | 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 founders, leaders and technical experts with experience in established or fast-growing tech companies, so as to contribute to the development of Singapore's tech ecosystem. Tech.Pass will allow pass-holders flexibility in the participation of activities such as starting and operating a business, being an investor, employee, consultant or director in one or more Singapore-based companies, mentoring start-ups and lecturing at local universities.

UPDATE AND TRENDS

Current developments

45 | 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.

simmons+simmons

Yingyu 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
Fax: +65 6831 5688
www.simmons-simmons.com

In early December 2020, MAS announced that four entities were awarded digital banking licences.

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 licence – 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 FATF standards.

South Korea

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

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

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

Innovative fintech startups are emerging in South Korea, and existing financial institutions are showing great interest in investing in fintech or making new business attempts.

To create momentum in the current trend, 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, and is introducing a number of reformatory measures to create a fintech-friendly regulator landscape. For example, the Electronic Financial Transactions Act is being amended in a direction to ease restrictions on electronic financial transactions and simplify the relevant licence requirements.

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 Bank 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 Financial Services Commission (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 (FISCMA). Under FISCMA, 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 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 (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. 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 regulate 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 Financial Consumer Protection Act, 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 FISCMA. FISCMA also regulates crowdfunding platforms. However, other alternative finance products and services, such as peer-to-peer (P2P) lending, are regulated under different regulations.

Alternative investment funds

8 | Are managers of alternative investment funds regulated?

The collective investment schemes and their managers are regulated under FISCMA. 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 FISCMA.

Peer-to-peer and marketplace lending

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

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 FISCMA. 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.

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.

Previously, FISCMA allowed only natural persons to provide investment advisory services. However, it has been amended to permit robo-advisers (eg, investment advisory by mechanical devices).

It should be, however, noted that such robo-adviser services are treated as the provision of 'investment advice' under FISCMA, subject to registration as an investment advisory service provider in principle.

In an exceptional case where another investment advisory service provider registered under FISCMA 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 Financial Consumer Protection Act.

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?

Passporting is not permitted in South Korea.

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.

In the past, the sales and marketing activities used to be regulated by different laws (eg, the Banking Act, the Financial Investment Services and Capital Markets Act) according to the type of business for which the sales and marketing activities are conducted. However, taking effect on 25 March 2021, the Financial Consumer Protection Act provides a uniform regulatory framework for all financial products and services.

More specifically, the Financial Consumer Protection Act applies the so-called '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, to inform the customer of such fact and then to 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 on 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 on 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
Prohibition on false or exaggerated advertisements	Refrain from making false or exaggerated advertisements

In addition, the Financial Consumer Protection Act 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.

CHANGE OF CONTROL

Notification and consent

20 | 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

21 | 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 Act on Reporting and Using Specified Financial Transaction Information. 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 (main criminal code of South Korea) and the Anti-Graft Act. As such, all the companies (including fintech startups) operating their business in South Korea must comply with such laws.

Guidance

22 | 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.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

In South Korea, an investor and a borrower do not directly enter into a loan agreement or security agreement for the peer-to-peer (P2P) lending with each other. Instead, P2P lending platforms, or the finance company that is a partner of the platform:

- receives the investment money from an investor;
- lends the money to the borrower designated by the investor; and
- grants to the investor the right to receive the principal and interest payments from such lending.

Therefore, the collection of loan claims and delivery to the investor are handled by P2P lending platforms and their partner financial companies.

Assignment of loans

24 | What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

Under the P2P Lending Act, the P2P lending platform or partner financial company lends money to the borrower and the investor receives the right to the principal and the interests accrued thereon.

P2P lending platforms and their partner financial companies may only transfer their claims against a borrower (namely, receivables) to the entities specified in the Lending Business Act, such as registered loan collection business entities, banks or credit specialised companies. Such transfers require either:

- prior notice to the borrower; or
- the borrower's consent to such transfer.

The notice or consent should be given in accordance with a deed bearing a fixed effectuation date (as may be provided by postal offices, registry, etc) to be effective against a third party.

Securitisation risk retention requirements

25 | Are securitisation transactions subject to risk retention requirements?

There are no risk retention requirements for securitisation transactions.

Securitisation confidentiality and data protection requirements

26 | Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

In general, special purpose companies are not permitted to purchase and securitise P2P or marketplace loans, unless they register their securitisation plan with the Financial Services Commission pursuant to the Asset-backed Securitization Act.

When special purpose companies purchase and securitise P2P or marketplace loans, they shall comply with data protection laws regarding the information relating to the borrowers if such information is provided.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 | 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 Financial Services Commission 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 addition, an entity that provides robo-advice services shall comply with relevant regulations under the Financial Investment Services and Capital Markets Act (FISCMA).

Distributed ledger technology

28 | 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.

For your reference, 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 as long as it complies with EFTA.

Cryptoassets

29 | 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 Information Act. Under the Financial Transaction Information Act, 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 Specified Financial Transaction Information Act 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.

Token issuance

30 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 be gradually expanded to other types of ICOs. On the other hand, given the high risk of losses and the breadth of investors to be affected, regulation of STOs is expected to be implemented via amendment of FISCMA, which provides for stricter investor protection

DATA PROTECTION AND CYBERSECURITY

Data protection

31 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 released the guidelines to be used as a reference by fintech companies in pseudonymising and anonymising personal credit data.

Cybersecurity

32 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 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 Financial Services Commission 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 system and information and communications network, 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

33 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 out 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 institution 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 of 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

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

To use cloud computing services in the financial services industry, cloud service providers must install all system servers including those used by their management systems within South Korean territory, comply with various monitoring regulations under the Regulation on Supervision of Electronic Financial Transactions, and submit a periodical compliance report to the Financial Supervisory Service.

Cloud computing services for the financial services industry must also establish either of the following to be exempted from anti-hacking network segmentation rules applicable to traditional financial service providers:

- it is essential to connect the internal communication network terminal with external institution to make it operational; or
- the remote access to the internal work system from a wide area network is enabled by communication network equipped with the same level of security as the leased line on the terminal with security function and available with registered devices only.

On 14 April 2022, the Financial Services Commission announced a plan to ease regulations related to the use of cloud computing services in the financial sector, by reducing compliance or monitoring burdens and expanding exemptions from anti-hacking requirements for development and testing servers starting from 2023.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

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

The source cord 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 a computer is specifically realised by using hardware (Supreme Court Decision 2007Hu256 rendered on 24 December 2008).

IP developed by employees and contractors

36 | 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

37 | 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

38 | 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

39 | 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

40 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, removal of facilities provided for infringement) as well as criminal punishment by filing a criminal complaint against the infringer.

COMPETITION

Sector-specific issues

41 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

42 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 startups 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
- 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.

bkl BAE, KIM & LEE

Juho Yoon
juho.yoon@bkl.co.kr

Young Ju Park
youngju.park@bkl.co.kr

Se Young Im
seyeong.im@bkl.co.kr

Jinhee Rhew
jinhee.rhew@bkl.co.kr

Centropolis B
26 Ujeongguk-ro
Jongno-gu
Seoul 03161
Korea
Tel: +82 2 3404 0000
www.bkl.co.kr

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

43 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

44 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?

Any foreigner is required to obtain a visa to qualify for employment in South Korea. Among the types of visas granted to foreigners, fintech operators may consider using E-7 as a status of stay for employment to hire skilled staff from abroad.

E-7 is a status of stay issued to foreigners who wish to work in areas specially designated by the Minister of Justice pursuant to the contract with a public or private organisation, and occupations such as finance and insurance expert, network system developer, data expert, web developer, information security expert, etc, have been designed as occupations eligible for the issuance of E-7 status of stay.

However, the Ministry of Justice has recently issued E-7 visas to workers engaged in emerging industries who meet the score-based requirements, even though they do not work in the previously designated areas, to attract more talent into new and growing industries.

Moreover, indispensable skilled workers who wish to engage in the management, administration, production and technical areas of a

foreign-invested company in accordance with the Foreign Investment Promotion Act are eligible to work in South Korea by acquiring a D-8 visa. Hence, fintech companies that have invested in South Korea may also consider recruiting foreign workers by using a D-8 visa.

UPDATE AND TRENDS

Current developments

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

There is discussion within the industry of potentially amending the Electronic Financial Transactions Act, which regulates any financial business conducted electronically, such as fintech, to introduce a new type of licence, namely, a 'comprehensive payment service provider' licence, which would allow fintech companies to issue accounts for receipt or withdrawal to customers. This would enable fintech companies to provide financial services such as cash deposits and withdrawals, transfers, remittances and payments on their own without having to affiliate with a bank. The South Korea Fintech Industry Association is acting as the main driver behind this industry-wide discussion, but it remains to be seen whether the new administration will be receptive to the foregoing idea.

The South Korean National Assembly is currently deliberating a bill (the Virtual Asset Industry Act) that aims to set out a comprehensive legal framework for the virtual asset industry. The bill includes, among other things, a registration and reporting scheme for virtual asset businesses (in harmonisation with the legislation already in place, namely, the Act on Reporting and Use of Certain Financial Transaction Information), greater disclosure obligations to protect investors, prohibition of unfair trade and sanctions in the case of violations.

Spain

Alfredo de Lorenzo, Álvaro Muñoz, Carmen Torres, Ignacio González, Juan Sosa, María Tomillo and Raquel Ballesteros

Simmons & Simmons

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 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
- 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 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 for 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 the second Markets in Financial Instruments Directive 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 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 the 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 the 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 (ie, 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 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 the Undertakings for Collective Investment in Transferable Securities Directive and the Alternative Investment Fund Managers Directive (AIFMD), in addition to the regime that applies specifically to Spanish CISs.

CISs are a regulated product in Spain and must be locally registered. Management and distribution of CISs (ie, 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 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 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 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 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 (ie, professional investors) and to €2 million for non-accredited investors;
- equity crowdfunding projects, which cannot exceed 125 per cent of the project's projected target; and
- 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 of the European Parliament and of the Council, of 7 October 2020, 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 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 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 of 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 the aforementioned Royal Decree 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 referred 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, agent or on a cross-border basis without 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.

SALES AND MARKETING

Restrictions

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

Investments

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 the Spanish Securities Market Law approved by the Royal Legislative Decree 4/2015, of 23 October (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 the Order EHA/1717/2010, of 11 June, of 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 which 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 MiFID), 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 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 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.

The Bank of Spain Circular 4/2020, Order 1718/2010, CNMV Circular 2/2020 and Order EHA 1717/2010 together with Law 10/2014, of 26 June, on management, supervision and solvency of credit institutions (Law 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 the General Law 34/1988, of November 11, on Advertising (Law 34/1988). The Spanish regulation governing advertising of banking products and services and the one governing advertising of investment products and services follow the same pattern.

The Bank of Spain Circular 4/2020 and the 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.

CHANGE OF CONTROL

Notification and consent

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

There are specific rules relating to 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

21 | 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.

On 29 April 2021, Royal Decree Law 7/2021 entered into force, amending Spanish Law 10/2010 on the prevention of money laundering and terrorist financing and implementing the Fifth AML Directive. The following developments shall be taken into account:

- new obliged entities:
  - virtual currency service providers for the exchange of fiat currencies and for 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);
- 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

22 | 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.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Spanish law does not generally impose any formal requirements for executing loans. An exception to this is in respect of consumer loans for which there is a requirement that the agreement has to be drawn up on paper or another durable medium. Electronically signed documents are recognised and are enforceable. The market practice, however, is that loan agreements are generally made in writing and are notarised by a Spanish public notary for the lenders to be able to enforce the loan through certain special summary foreclosure procedures for notarised agreements. Only loans of small amounts are not executed in this way.

Security agreements, on the other hand, are subject to strict formalities and they will not be enforceable if these formalities are not met. All security agreements (with the exception of financial collateral arrangements) have to be notarised and certain other formalities are required depending on the type of security. Real estate mortgages have to be registered with the land registry. In the case of ordinary pledges, the possession of the charged asset has to be delivered to the creditor or to someone acting on its behalf. Pledges over shares, claims or bank accounts have to be notified to the company, the debtor or the account bank, respectively.

Assignment of loans

24 | What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

Under Spanish law, the transfer of a loan originated on a peer-to-peer (P2P) marketplace lending platform requires only the agreement of the transferor and the transferee. The loan agreement could impose additional requirements that would then be required for the effectiveness of the assignment in relation to the borrower, but this is not customary except in large loans. The transfer is valid even if no notice is given to the borrower. However, until this notice is given, or the borrower is aware of the transfer, the transfer is not effective against the borrower and he or she may discharge his or her obligations by payment to the transferor, without any liability to the transferee. In addition, the transfer will not be fully effective against third parties (including the transferor's creditors) unless the transfer agreement is executed and notarised with the intervention of a public notary. As a result, transfer agreements are usually notarised, and the parties notify the transfer to the borrower as soon as it is effective.

Any security interest that secures the loan will transfer automatically with the loan and will secure the new creditor. In practice, however, it is necessary to carry out certain additional acts to put the security under the name of the new lender. In the case of mortgages, it is necessary to register the transfer in the land registry and in the case of pledges over shares, claims or bank accounts, notice should be given to the company, the debtor or the account bank respectively.

Securitisation risk retention requirements

25 | Are securitisation transactions subject to risk retention requirements?

Application of the EU risk retention rules to securitisations of loans originated on a peer-to-peer or marketplace lending platform (P2P securitisations)

The risk retention requirements set out in the sectoral EU legislation will apply to P2P securitisations that are offered to European banks, investment firms, alternative investment funds or insurers. Under the current sectoral EU risk retention rules, certain investors (such as credit institutions, Markets in Financial Instruments Directive-regulated firms and alternative investment fund managers) will be subject to higher regulatory capital charges where they invest in securitisation positions that do not comply with the risk retention rules. Those rules require that either the sponsor, originator or original lender in respect of the securitisation explicitly discloses to the investor that it will retain, on an ongoing basis, a material net economic interest in the securitisation (which in any event is not less than 5 per cent) using one of five prescribed retention methods. Those methods include (among other things) retention of:

- the most subordinated tranche or tranches, so that the retention equals no less than 5 per cent of the nominal value of the securitised exposures;
- 5 per cent of the nominal value of each of the tranches sold to investors; or
- randomly selected exposures equivalent to no less than 5 per cent of the nominal value of the securitised exposures. The definitions of 'sponsor' and 'originator' as used in the sectoral EU legislation are set out in the legislation. The term 'original lender' is undefined.

The risk retention rules set out in the sectoral EU legislation have been replaced as of 2 January 2019 with the risk retention rules set out in the EU Securitisation Regulation. The retention requirement and the methods of retention remain the same under the EU Securitisation Regulation. However, there is now a direct requirement on the sponsor, originator and original lender to agree on an entity that will act as retention holder and to ensure compliance with the retention requirement. In the absence of agreement among the originator, sponsor or original lender as to who will be the retention holder, the originator will be the retention holder. Definitions of 'sponsor', 'originator' and 'original lender' are set out in the EU Securitisation Regulation.

The EU Securitisation Regulation does not explicitly set out the jurisdictional scope of the 'direct' retention obligation, but there is a helpful note in the Explanatory Memorandum to the European Commission's original proposal for the EU Securitisation Regulation that the intention is that the direct approach would not apply to securitisations (including P2P securitisations) where none of the originator, sponsor or original lender is 'established in the EU'. 'Establishment' is typically described by reference to the jurisdiction in which the legal entity is incorporated or has its registered office. Therefore, the non-EU subsidiary of an EU entity may not be subject to the direct retention obligation because a subsidiary is typically a separate legal entity, whereas a non-EU branch of an EU entity may be caught within this provision because a branch is typically not a separate legal entity. Market participants are still seeking clarity on this, and it is expected that this point will be raised as part of the ongoing European Banking Authority (EBA) consultation on risk retention.

Possible retaining entities in respect of P2P securitisations

Typically, a P2P lending platform will not qualify as the sponsor, originator or original lender of a P2P securitisation, and another entity with the capacity to retain will therefore need to be identified. The range of entities with capacity to retain is broader under the EU Securitisation Regulation than under the current EU sectoral legislation and, therefore, the ability of an entity to retain will depend on the rules that apply at the time the securitised notes are issued. Any entity that retains in the capacity of originator is expected to be an entity of substance, and the EU Securitisation Regulation expressly provides that an entity shall not be considered to be an originator where it has been established or operates for the sole purpose of securitising exposures. The EU Securitisation Regulation does not specify in what circumstances an entity will be considered to have been established for the sole purpose of securitising exposures but, in December 2017, the EBA published a consultation paper that proposed that an originator will not be considered to have been established with the 'sole purpose' of securitising exposures if it satisfies certain conditions, including that:

- it has a broader business enterprise and strategy;
- it has sufficient decision makers with the required experience; and
- its ability to make payment obligations depends neither on the exposures to be securitised nor on any exposures retained for the purposes of the risk retention regulations.

Securitisation confidentiality and data protection requirements

26 | Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

The entity assigning loans to the special purpose vehicle (SPV) must ensure that there are no confidentiality requirements in the loan documents that would prevent it from disclosing information about the loans and the relevant borrowers to the SPV and the other securitisation parties. If there are these restrictions in the underlying loan documentation, the assignor will require the consent of the relevant borrower to disclose to the SPV and other securitisation parties the information they require before agreeing to the asset sale. In addition, the SPV will want to ensure that there are no restrictions in the loan documents that would prevent it from complying with its disclosure obligations under Spanish and EU law (such as those set out in the Credit Rating Agency Regulation). Again, if these restrictions are included in the underlying loan documents, the SPV would be required to obtain the relevant borrower's consent to this disclosure. In addition, if the borrowers are individuals, the SPV, its agents and the P2P platform will each be required to comply with the statutory data protection requirements under Spanish law.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 | 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 the 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.

Distributed ledger technology

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

No.

Cryptoassets

29 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 7/2021 entered into force, implementing the Fifth AML Directive and amending certain provisions of Law 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 AML legislation. Crypto-asset 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 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

30 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 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 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 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. Its aim is 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 crypto-asset 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 crypto-asset, 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:

- crypto-asset service providers when they engage in crypto-asset 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 in 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 in order 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.
- 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, 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.

Furthermore, in September 2020, the European Commission made a proposal for regulation of the cryptoassets market (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 crypto-asset would be electronic money). However, a large part of the cryptoassets typology is not framed within said regulation.

In this sense, the aim of the MiCA Proposal is 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.

Some cryptoassets are considered as 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 in 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.

The European Commission must present to the European Parliament and the Council of the EU, before 1 January of 2025, a legislative proposal to modify the taxonomy regulation.

Given the complexity of the phenomenon, criteria in this regard are subject to review in light of the experience accumulated and the debate that is currently taking place at an international level and, in particular, within the European Securities and Markets Authority. The CNMV and Bank of Spain are jointly working on this topic, setting out criteria applying in relation to ICOs. There is an official document that provides guidance on, mainly, the consideration of tokens as transferable securities, the need and scope of intervention of entities authorised to provide investment services, as well as representation of tokens and the consequence of their trading on trading platforms, and, finally, the requirement for a prospectus.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 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 EU General Data Protection Regulation (GDPR) came into force with direct effect across the entire EU. In Spain, additionally, domestic law (Organic Law 3/2018, of 5 December, on the protection of personal data and guarantee of digital rights (SLDP)) was enacted and came into effect from 7 December 2018. Likewise, among other 'domestic peripheric regulations', one of them that plays an important role in the field of processing personal data within the fintech sector is Law 34/2002, of July 11, on services of the information society and electronic commerce (LSSIyCE).

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 3, 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 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and domestic regulation). 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/standard (article 6) or special (article 9 in relation to article 6)). Additionally to the lawful basis, the GDPR requires a mandatory obligation in order 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 (DPO). 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 (as an example, the last administrative fine imposed by the AEPD on Google LLC amounted to €10 million).

Cross-border processing of data falls under the legal framework of 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 Liechtenstein, Iceland and Norway, as they are part of the European Economic Area) is caught by provisions 44–49 of the GDPR, as explained below:

- Article 45 – adequacy decision: the European Commission may recognise through its adequacy decisions relating to some or all of the third countries to which you are about to transfer personal data that they offer an adequate level of protection, similar to the European Union.
- Article 46 – appropriate safeguards: in the absence of an adequacy decision, international transfers of personal data may be carried out with any of the following guarantees:
    - a legally binding and enforceable instrument between public authorities or bodies;
    - binding corporate rules;
    - standard data protection clauses (SCCs) adopted by the European Commission (Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance);
    - SCCs adopted by a supervisory authority and approved by the European Commission;
    - codes of conduct, together with binding and enforceable commitments of the controller or processor in the third country to implement appropriate safeguards, including those relating to the rights of data subjects; and
    - certification mechanisms, together with binding and enforceable commitments of the controller or processor in the third country to implement appropriate safeguards, including those relating to the rights of data subjects.
- Article 49 – specific situations: in the absence of an adequacy decision and appropriate safeguards, international transfers may only be carried out if one of the following conditions is met:
    - the data subject concerned has explicitly given his or her consent;
    - the transfer is necessary for the performance of a contract between the data subject and the controller or for the performance of pre-contractual measures taken at the request of the data subject;
    - the transfer is necessary for the conclusion or performance of a contract, in the interest of the data subject, between the controller and another natural or legal person;
    - the transfer is necessary for important public interest reasons;
    - the transfer is necessary for the establishment, exercise or defence of 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 his or her consent; and
    - the transfer is made from a public register that, under Union or member state law, is intended to provide information to the public and is open to inspection by the public in general or by any person who can establish a legitimate interest, but only insofar as the conditions for inspection laid down by Union or member state law are met in each individual case.

Note that the judgment of the Court of Justice of the EU known as *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, even though it is expected that both parties will come to an agreement 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 chosen for 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 EU.

Cybersecurity

32 | 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 12/2018, of 7 September, which was amended by Royal Decree 43/2021, of 26 January.

With regard to sector standards, a public body – the National Institute of Cybersecurity (INCIBE) – 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

33 | 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 (IOT). However, depending on the activities contemplated, consideration will need to be given to the processing of personal data under the General Data Protection Regulation and Organic Law 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 1/1996, of 12 April (the Copyright Law), and parts of the General Telecommunications Law 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 the Securities Market Law.

Cloud computing

34 | 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 entitled '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 throughout 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

35 | 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 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 as '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 relation between employer and employee, the two main ways of obtaining moral and exploitation rights derived from software are: (1) creation (original owner); (2) assignment or license of exploitation rights (derivative owner), but in this last scenario the original creator will keep the moral rights as such rights cannot be assigned or licensed under the Copyright Law.

IP developed by employees and contractors

36 | 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 (1) during the course of his or her role in the company and (2) 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, 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

37 | 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 (see, by way of example, 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.

Speaking of copyright, 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

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

The Trade Secrets Directive has been implemented in Spain by means of Law 1/2019, of 20 February, on trade secrets (the Trade Secret Law). Therefore, to benefit from trade secret protection three requisites shall be met (confidential, business value by virtue of its secrecy and adequate measures implemented to keep it confidential).

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

39 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 EU (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

40 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 by an injured party.

Regarding IP, the injured party is entitled, among others, to take measures before local or European offices (see, by way of example, in the field of trademarks through annulment action or expiry due to lack of use action), file preventive letters (in order 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 Commercial Court No. 8, dated 25 February 2020) and, obviously, they are entitled to file legal actions before the courts with or without interim measures or preliminary measures.

COMPETITION

Sector-specific issues

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

No.

TAX

Incentives

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

On December 2021, the Spanish government submitted for parliamentary processing the Bill to promote the start-up ecosystem (the Bill). If approved, the Bill will incorporate new tax incentives for start-up companies:

- a reduced CIT 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

43 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. In the last budget bill (Law 22/2021) a minimum of 15 per cent effective tax rate in corporate tax for large companies (net turnover of more than €20 million) has been implemented. This minimum effective taxation requirement in practice operates as a limit to apply different tax credits, including R&D and IT tax credits mentioned above.

On top of that, from 1 January 2021, the participation exemption is limited to only 95 per cent of the relevant income.

In addition, during 2021, the following taxes have been approved.

Digital services tax

A digital services tax, as an indirect tax assessed on a quarterly basis. The taxable event is the provision of certain digital services in Spain such as the sale of online advertising space, online intermediary services and the transfer of user-related data gathered from digital platforms. The tax rate is 3 per cent of gross revenue.

Financial transaction tax

The government decided to unilaterally propose a local financial transaction tax (FTT) given the lack of real progress of the enhanced cooperation procedure for the adoption of an FTT. It has been implemented as an indirect tax. The taxable events for the financial transactions tax are:

1 the acquisition of qualifying shares of Spanish companies (ie, shares listed on a regulated Spanish or EU stock exchange with a market capitalisation as at 1 December of the year before the acquisition exceeding €1 billion);
2 the acquisition of securities corresponding to depositary receipts representing qualifying shares; and
3 the acquisition of qualifying shares or securities (as provided in (1) or (2)) derived from the execution or settlement of convertible or exchangeable notes or bonds, financial derivatives, any financial instruments or certain financial agreements.

The tax basis is defined as the consideration for acquisitions subject to the tax. The tax rate would be 0.2 per cent.

IMMIGRATION

Sector-specific schemes

44 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 professional (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 €45,000. 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

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

There are no relevant developments to note. From time to time, the Spanish Securities Market Commission updates a question-and-answer document answering the most relevant questions raised by the industry in Spain. In addition, there is now a guide to be followed by entities interested in submitting their projects through the Spanish sandbox, which was finally approved by means of Law 7/2020 of 13 November, for the transformation of the financial sector. In June 2021, the General Secretariat of the Treasury and International Financing published a resolution by means of which access to the sandbox is open to receive requests. Since June 2021, there have been two additional announcements in order to receive requests. The current announcement ended on 1 March and the Resolution approving the projects regarding the sandbox was issued on 15 June 2022.

Alfredo de Lorenzo
alfredo.delorenzo@simmons-simmons.com

Álvaro Muñoz
alvaro.munoz@simmons-simmons.com

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 Ángel 11
5th floor
28010 Madrid
Spain
Tel: +34 91 426 2640
Fax: +34 91 578 2157
www.simmons-simmons.com

Sweden

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

Vinge

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, Lendify, 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. This phenomenon may indicate a structural change in loan origination in Sweden and a reduced market share for Sweden's largest banks. However, the Swedish Financial Supervisory Authority (SFSA) has indicated plans to introduce additional regulations in this area, and the longevity of the new market actors remains to be seen. The SFSA has recently increased its focus on consumer lending and credit assessment.

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, on several occasions, expressed interest in supporting and promoting the development of the Swedish fintech sector. While the former Minister for Financial Markets supported the idea of setting up regulatory sandboxes where fintech startups may develop in an unregulated environment or only comply with a regulation-light regime, but the SFSA disagreed and proposed the introduction of the SFSA Innovation Centre. The Innovation Centre was opened in 2018 and 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 startups.

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 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 Capital Requirements Regulation No. 575/2013.

Further, a licence is required for offering the services and products covered by Markets in Financial Instruments Directive 2014/65/EU (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;
- 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 Capital Requirements Regulation No. 575/2013) or the Housing Credit Operations Act (2016:2014) (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.

On 1 July 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 the Alternative Investment Fund Managers Directive 2011/61/EU (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.

While there is currently no specific regulation of crowdfunding services under Swedish law, certain crowdfunding schemes may fall within the scope of the general financial services framework. However, Regulation (EU) 2020/1503 on Crowdfunding Service Providers (the Crowdfunding Regulation) entered into force on 10 November 2020 and will apply from 10 November 2021, establishing 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.

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.

Payment services

12 | Are payment services regulated in your jurisdiction?

Yes. Payment services are regulated under the Second Payment Services Directive (EU) 2015/2366 (PSD 2), which has been implemented into Swedish law through the PSA. Money remittance, execution of payment transactions, acquisition of payment instruments, payment initiation and account information services are among the services currently regulated under the PSA.

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. Payment services are regulated under PSD 2, which has been implemented into Swedish law through the PSA. Money remittance, execution of payment transactions, acquisition of payment instruments, payment initiation and account information services are among the services currently regulated under the PSA.

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).

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 on 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).

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 Practices 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.

CHANGE OF CONTROL

Notification and consent

20 | 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 CEO 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

21 | 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 (SMA).

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

22 | 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.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Loan and security agreements are subject to the general Swedish contract laws and principles. At a basic level, both parties would therefore normally have to agree on the terms and conditions of the agreement in question. There are no rules hindering the execution of agreements electronically, but the Swedish Enforcement Agency does not accept electronic negotiable promissory notes as a basis for enforcement actions.

Assignment of loans

24 | What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

Perfection of an assignment against third parties depends on whether the loan is represented by a negotiable promissory note or a non-negotiable promissory note. In the former scenario, the promissory note must be transferred to the assignee, whereas in relation to non-negotiable promissory notes, the borrower must be notified of the assignment so that the debtor can solely make its payments to the assignee with discharging effect.

In the event the assignment is not perfected, the loan would be included in the bankruptcy estate of the assignor in relation to which the assignee would only have a non-secured claim.

Securitisation risk retention requirements

25 | Are securitisation transactions subject to risk retention requirements?

Perfection of an assignment against third parties depends on whether the loan is represented by a negotiable promissory note or a non-negotiable promissory note. In the former scenario, the promissory note must be transferred to the assignee, whereas in relation to non-negotiable promissory notes, the borrower must be notified of the assignment so that the debtor can solely make its payments to the assignee with discharging effect.

In the event the assignment is not perfected, the loan would be included in the bankruptcy estate of the assignor in relation to which the assignee would only have a non-secured claim.

Securitisation confidentiality and data protection requirements

26 | Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

Provided that the company processes personal data as part of its operations it would, in respect of borrowers' personal data, be subject to the EU General Data Protection Regulation and Swedish data protection laws.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 | 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 (SMA) and is consequently subject to all the substantive provisions of the Swedish Markets in Financial Instruments Directive 2014/65/EU implementation, 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 the General Data Protection Regulation (GDPR).

Distributed ledger technology

28 | 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 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 the GDPR and Swedish data protection laws will be applicable.

Cryptoassets

29 | 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 Cryptoassets.

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 the Fifth Anti-Money Laundering Directive (EU) 2018/843, 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 SMA, the Electronic Money Act (2011:755) (EMA) or the Payment Services Act (2010:751) (PSA) could apply.

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

30 | 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.

DATA PROTECTION AND CYBERSECURITY

Data protection

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

The 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 whistleblowing 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);
- 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

32 | 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

33 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) (SMA);
- the Electronic Money Act (2011:755);
- the Payment Services Act (2010:751);
- the Swedish Financial Supervisory Authority (SFSA) regulations;
- detailed provisions set out in 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

34 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

35 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. 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

36 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.

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.

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

37 | 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

38 | 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

39 | 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 Practices Act (2008:486) (MPA). 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

40 | 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

41 | 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

42 | 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

43 | 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

44 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

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

According to the Stockholm Fintech Guide, Stockholm received 18 per cent of all private placements in fintech companies across Europe between 2013 and 2018, and around 400 fintech companies are active in Stockholm, as compared to the end of 2017 when there were around 150.

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 has been appointed to investigate a general transition towards the digitalisation of currency in Sweden and will publish its statement on 30 November 2022 at the latest. Sweden in general – and Stockholm in particular – are vibrant for fintech companies, and the coming years may provide for further developments on the Stockholm fintech scene.

Following recent developments in the global financial markets, it has proven more difficult for fintech firms and startups to raise capital. This may eventually lead to more consolidations and an increased focus on cost savings rather than expansion.

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
Box 1703
111 87 Stockholm
Sweden
Tel: +46 10 614 30 00
www.vinge.se

Switzerland

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

Homburger

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 as well as the Swiss Financial Market Supervisory Authority (FINMA) recognise the potential that fintech and blockchain technology offer to the Swiss financial services industry as well as 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 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 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 (FMIA) and certain clarifications relating to the treatment of cryptocurrencies in Swiss insolvency proceedings.

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 the communal, cantonal and federal level. 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?

Whether or not specific business activities performed by a fintech company qualify as a regulated activity in Switzerland will need to be determined 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 (FBO), the acceptance and storage of cryptoassets as well as related custody services are also deemed 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, since 1 January 2019, the FBA has provided 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, provided that the deposits 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 (1) dealing in securities in its own name but on its clients' account; (2) dealing in securities on a short-term basis on its own account and thereby either (a) impacting systemic stability of the Swiss financial market or (b) being directly admitted to a trading venue within the meaning of the Financial Market Infrastructure Act (FMIA); or (3) market making activities. In light of the outlined legal framework, fintech companies will typically require a licence as a securities dealer, if their business model includes trading of digital assets, qualifying as 'securities' within the meaning of the FMIA, for the account of its 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 asset tokens or futures contracts on cryptocurrencies, and are suitable for mass trading, such digital assets will qualify as securities.
- 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. It should also be noted that trading venues domiciled outside Switzerland require a recognition by FINMA, if they admit Swiss supervised entities to their trading facilities. Finally, in 2021 a new licence category, 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 subject to the duty (1) to become a member of a self-regulatory organisation; (2) to determine the identity of the contracting party and the beneficial owner of the transferred assets; and (3) 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 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 (1) ensure an irreproachable conduct of business operations in Switzerland; (2) have sufficient education and experience in the area of financial services; and (3) have adequate liability insurance or provide respective securities. Further, the credit provider must hold Common Equity Tier 1 capital in the amount of 8 per cent of the credit outstanding in Switzerland, or at least 250,000 Swiss francs, whichever is higher.

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 (1) 100 million Swiss francs or (2) 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 (1) to become a member of a self-regulatory organisation; (2) to determine the identity of the contracting party and the beneficial owner of the transferred assets; and (3) 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 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 July 2020, FINMA published a fact sheet on crowdfunding and provided guidance on the regulatory treatment of crowdfunding platforms. Pursuant to FINMA's guidance, as 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 (in order, 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 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?

The European Payment Services Directive 2 (PSD2) is not applicable in Switzerland. Under the FMIA, an entity that operates a payment system (ie, a facility that clears and settles payment obligations based on uniform rules and procedures) is subject to a licensing requirement in Switzerland, provided (1) the licensing requirement is necessary for the proper functioning of the Swiss financial market or the protection of financial market participants; and (2) 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. The Swiss National Bank also has the competence 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, most fintech companies providing payment services will 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 regulation 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 in order 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 (ie, 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 strictly regulated under the ISA. Therefore, 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. Furthermore, 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/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).

CHANGE OF CONTROL

Notification and consent

20 | 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.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

21 | 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: (1) accept or hold deposit assets belonging to third parties; (2) assist in the investment of such assets; or (3) 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/ICOs: 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 subject to the AMLA if such services are provided in the context of a permanent business relationship.

Guidance

22 | 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) 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'.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Except for consumer credits governed by the Federal Act on Consumer Credits, a loan agreement need not be executed in writing in order to be enforceable (but note that a written acknowledgment of debt by the debtor may enable the creditor to accelerate debt collection and enforcement proceedings in Switzerland). Lenders should nevertheless ensure that they obtain a sufficiently clear evidentiary record of the loan.

Regarding security agreements, form requirements apply. A pledge under Swiss law is valid only if the agreement is entered into in writing (ie, with wet-ink or Swiss-law qualified electronic signature of the pledgor). An agreement for security in the form of real property (ie, mortgages) must be executed as a public deed.

An assignment of claims (including for security purposes) is also valid only if executed in writing by the assignor with wet-ink or Swiss-law qualified electronic signature.

Assignment of loans

24 | What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

Claims arising under a loan may be assigned unilaterally and notification of the borrower owing the respective claim is not a perfection requirement (but omission of such a notification creates the risk that the borrower discharges the debt and extinguishes the assigned claim by performance to the original creditor or assignor).

An assignment of claims (including for security purposes) is also valid only if executed in writing by the assignor with wet-ink or Swiss-law qualified electronic signature.

Securitisation risk retention requirements

25 | Are securitisation transactions subject to risk retention requirements?

The EU Securitisation Regulation does not apply in Switzerland and its rules are not part of the Swiss regulatory framework.

Securitisation confidentiality and data protection requirements

26 | Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

Subject to the terms and nature of the contractual agreements between the originator of the loan and the borrower, the standard of confidentiality owed to the borrower is generally set by whether the originator is merely subject to the general data protection requirements imposed by the Swiss Data Protection Act or, for example, as a bank or other Swiss-licensed financial institution, additional statutory secrecy obligations. Absent a waiver of confidentiality by the borrower, the originator must ensure that the SPV complies with the respective data protection and confidentiality standard. Furthermore, a transfer of data abroad may be subject to additional limitations.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 | 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 on '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 in order 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 (ie, 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 – qualifies 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.

Distributed ledger technology

28 | 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 enable 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

29 | 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: (1) Swiss securities firm licence requirements under the FinIA; (2) Swiss trading platform regulations under the FMIA; and/or (3) 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) are 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 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 are 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 (1) whether a single underlying or a basket of underlyings is used; (2) the type of underlying; as well as (3) if the stablecoin in question gives the holder a contractual redemption claim with regard to the underlying(s), respectively, the value of the underlying(s), or if the token merely fulfils the function of evidencing an ownership position with regard to the underlying(s).

As a third factor, the Federal Anti-Money Laundering Act (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.

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).
- 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 subject to the AMLA if such services are provided in the context of a permanent business relationship.

Token issuance

30 | 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: (1) Swiss securities firm licence requirements under the FinIA; (2) Swiss trading platform regulations under the FMIA; and/or (3) 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) are 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 FINMA. The question 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 FinSA, we believe that the question should be answered in the negative).
- Utility tokens are 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/ICO, according to FINMA, issuing cryptocurrencies (eg, payment tokens or stablecoins) constitutes financial intermediation (issuance of a means of payment).

DATA PROTECTION AND CYBERSECURITY

Data protection

31 | 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

32 | 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 (ie, to prevent unauthorised processing of such personal data).

In addition, for certain regulated businesses, additional requirements under applicable financial markets regulation applies: for instance, banks are subject to the FINMA Circular 2008/21 on Operational Risks (which is currently being revised), which stipulates certain requirements applicable to electronic client data. In addition, FINMA has issued Guidance 05/2020 detailing FINMA's expectation in relation to the reporting of cyber attacks by supervised financial institutions.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

33 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 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

34 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, the FINMA Circular 2018/3 on Outsourcing, the FINMA Circular 2008/21 on Operational Risks as well as general data protection law.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

35 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 (ie, if it is an intellectual creation with individual character). Thus, there is no need for the author of 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

36 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 to 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

37 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

38 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

39 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 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

40 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

41 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; an appeal has been lodged to the Federal Supreme Court, which is expected to provide its judgment in the course of 2022. In the area of merger control, the 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

42 | 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 VAT 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 VAT 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

43 | 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).

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
8005 Zurich
Switzerland
Tel: +41 43 222 10 00
www.homburger.ch

IMMIGRATION

Sector-specific schemes

44 | 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 EU. Furthermore, 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 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

45 | 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 in 2021 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 (DeFi) expanding their offerings in Switzerland.

Taiwan

Abe T S Sung and Eddie Hsiung

Lee and Li Attorneys at Law

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 below:

- 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 API connections;
- to provide the 'fund exchange' service by means of blockchain technology;
- to shorten the fund transmission gap by means of '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 ETFs using dollar cost averaging strategy based on the advice provided by robo-advisors.

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 a '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' (ie, 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 authority 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 for 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 loan, subject to (2) above, 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 future 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 record.

According to the P2P Self-Disciplinary Rules, banks may work together with the 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 the 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 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 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$50,000 for each subscription, and may not exceed NT$100,000 in aggregate in a year, except for in the case of 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 crowdfunding 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 loan, subject to (2) above, 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 (1) collecting and making payments for real transactions as an agent; and (2) accepting deposits of funds as stored value funds; the new business (3) 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 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 electronic 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 advocate of 'open banking' from some industry experts and market players, the FSC has demanded the Bankers Association to 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, to ask 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.

The FSC, as reported, adopts a three-phase approach for open banking. Phase I of 'open banking' was launched in late 2019, to allow public products information to be searchable by third parties (ie, 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 API 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-Adviser) (the Robo-Adviser Rules), which was approved by the FSC. Pursuant to the Robo-Adviser 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-Adviser Services; and
- customers should be informed of precautions before using Robo-Adviser Services.

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 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 to 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 include 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.

CHANGE OF CONTROL

Notification and consent

20 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 per cent, 25 per cent or 50 per cent of the voting shares of a bank;
- securities firm: no prior approval from the FSC is required;
- 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 (SICEs): no prior approval from the FSC is required.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

21 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, in order 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 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 (NTDs), 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 cryptoassets 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.

Furthermore, 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 anti-money laundering requirements applicable to financial institutions.

Guidance

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

No.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

There are no particular formality requirements for executing loan agreements. As to security agreements, under Taiwan law, different types of asset are subject to different formality requirements for perfection of a security interest created over them. The formality requirements for the most commonly seen security interests are as follows.

- Chattels: there must be a written agreement to create a chattel mortgage. The mortgagor needs not deliver the possession thereof to the mortgagee; however, a registration with the competent authority will be necessary for the mortgagee to claim the chattel mortgage against a bona fide third party.
- Real properties: security interest over real properties is taken by way of a mortgage registered with the relevant land registration offices. The parties must enter into a written agreement to agree on the creation of the mortgage and apply for registration of the mortgage before the mortgage can take effect.
- Shares: to create a pledge over shares, the pledgor and pledgee should enter into a written agreement. If the shares are represented by physical certificates, the pledged share certificates should also be duly endorsed by the pledgor and physically delivered into the pledgee's possession. A notice of pledge to the issuing company is also required. If the shares are listed and deposited to or registered with the local securities depository (ie, the Taiwan Depositary and Clearing Corporation (TDCC)), the above endorsement, physical delivery of the shares and notification to the issuing company are not required; instead, a pledge registration of the shares in the TDCC's book-entry system in accordance with the TDCC's regulations will suffice.

No different rules apply to cases of peer-to-peer lending.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

An assignment will not be effective against the borrower until the borrower has been notified of this assignment. If the borrower is not notified of the assignment, the borrower may still make the repayment to the assignor and discharge its repayment obligation by doing so.

Securitisation risk retention requirements

25 | Are securitisation transactions subject to risk retention requirements?

There are no mandatory risk retention requirements for securitisation as prescribed for in the Financial Asset Securitisation Act of Taiwan.

Securitisation confidentiality and data protection requirements

26 | Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

Personal information is protected by the Personal Data Protection Act (PDPA) and the collection and use of any personal data is subject to notice and consent requirements. If a special-purpose company, when purchasing and securitising loans, acquires any personal data, it will be subject to the obligations under the PDPA.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 | 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 played an important role. The 5+2 Plan mainly focuses on seven industries (ie, 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.

Nevertheless, the development of the application of artificial intelligence in financial business in Taiwan is still at a preliminary stage. The main application involves correspondence with clients, such as through Chatbot and Robo-Adviser Services.

Distributed ledger technology

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

No.

Cryptoassets

29 | 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 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 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, collectibles, 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

30 | 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 (ie, 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 security token

offerings (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 Sandbox Act and, if the experiment has a positive outcome, should be conducted pursuant to the SEA. Please see below for a summary of certain other major provisions of the STO Rules (ie, for STOs of NT$30 million or less):

- 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 Taiwan Stock Exchange or 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 – currently, only 'professional investors' are eligible to participate in STOs; where the professional investor is a natural person, the maximum subscription amount is NT$300,000 per STO. Nonetheless, the FSC issued a press release in January 2022 (the 2022 press release) that it plans 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 be 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 the 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 in the amount of NT$10 million.
  - Total offering amount capacity – the total offering amount of all STOs on a single platform should not exceed NT$100 million. A platform can accept to process a second STO only one year after the security tokens of the first STO have been traded on the platform. Pursuant to the 2022 press release, which also sets forth the plan for amending the STO Rules, the TPEx amended the STO rules on 21 January 2022, increasing the total offering amount capacity of all STOs on a single platform from NT$100 million to NT$200 million. Also, a platform is allowed to process a second STO six months after the security tokens of the first STO have been traded on the platform.
  - 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 statement 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.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 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

32 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, 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 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

33 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 the 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 Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation 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 the 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

34 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.

According to the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation 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 the 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).

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

35 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

36 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

37 | 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

38 | 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

39 | 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 by 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

40 | 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 willful act of misconduct, the court may 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
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

41 | 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

42 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

43 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

44 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.

UPDATE AND TRENDS

Current developments

45 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.

理律法律事務所
LEE AND LI
ATTORNEYS-AT-LAW

Abe T S Sung
abesung@leeandli.com

Eddie Hsiung
eddiehsiung@leeandli.com

8F, No. 555, Sec 4, Zhongxiao E Road
Taipei 11072
Taiwan
Tel: +886 2 2763 8000
Fax: +886 2 2766 5566
www.leeandli.com

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. 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. On 18 April 2022, the FSC announced draft amendments to the relevant regulations to set forth the requirements for establishing digital-only insurance companies and the draft amendments to relevant regulations for insurance solicitation, underwriting and claims settlement. It is expected that some of the market players (ie, existing insurance companies and technology companies) will apply to be digital-only insurance companies after the above amendments to the laws and regulations are officially promulgated and announced.

Turkey

Cigdem Ayozger Ongun and Deniz Erkan
SRP Legal

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

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

There is a dynamic fintech climate in Turkey and all areas of the market are ripe for investment. The fintech ecosystem in Turkey in 2022 is very active with 520 fintech companies actively operating as of today. Also, in the Turkish Fintech Ecosystem Status Report 2021, it is stated that there are 70.3 million active retail digital banking users and 1.7 million point-of-sale terminals, 52,000 automated teller machines, 82.8 million credit cards and 54.4 million prepaid cards in Turkey. The contactless payment rate reached 48 per cent. It is also noted that in the ecosystem in which 520 fintech companies actively operate, more than US$64 million worth of investments were made in 2021, and fintechs authorised in 2021 sold a total of US$48 million worth of shares in 2021.

In the Turkish fintech ecosystem, there are services (namely, payment and e-money services, money transfer and remittance, bill payment and system operator services) that are regulated under Turkish law, while others (namely, lending and credit scoring, digital wallet and application programming interface providers) are not. However, in less than a year, new regulations with regard to 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 in 12 March 2021, some of the legal regulations in this area were implemented in 2021. In this scope, the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers and the Communiqué on Information Systems of Payment and Electronic Money Institutions and Data Sharing Services in the Field of Payment Services Providers were published in the Official Gazette, dated 1 December 2021.

In addition, in the Turkish Fintech Ecosystem Status Report 2021, which was prepared by the Presidency Finance Office and published on 29 December 2021, it was emphasised that the National Fintech Strategy Document is planned to be published in the later months of 2022.

To strengthen the position of Istanbul Finance Center as a global fintech centre, a regulation experiment area (Sandbox) in the field of payments will be established by the second half of 2022. Moreover, fintech start-ups will be supported by the finance and technology base that is to be established in the Istanbul Finance Center.

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 government and regulators provide support to financial innovation; however, this support is not specifically financial industry-based. The support is provided to entities that meet specific criteria. 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 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 Programme (Communiqué No. 30892).

Latest developments concern Communiqué No. 30892: its amendments were published in Official Gazette No. 30969, effective from 5 December 2019.

Investment incentives are provided to all entities that meet the requirements pursuant to the above-mentioned laws and regulations. One of the purposes of the incentives is to support high- and medium-high technology investments that will provide technological transformation. Unlike many information technology or e-commerce projects, fintech projects are more likely to benefit from R&D 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. Moreover, the Presidential Decree on State Incentives Provided to Investments, which entered into force on 7 August 2019, saw a recent amendment that scrapped large-scale infrastructure project investments from the incentive regime and introduced increased incentives for R&D activities and value-added technology production.

Besides this, government support may be seen in the 11th Development Plan of Turkey (the 11th Plan), which was published in the Official Gazette, dated 23 July 2019. The 11th Plan includes objectives directly related to the Turkish financial technology ecosystem.

According to Presidential Decree No. 2834, published in Official Gazette No. 31207, dated 8 August 2020, from 8 August 2020, the rate of Bank and Insurance Transactions Tax (BITT) is applied as zero 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

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 the EU Payment Services Directive 2 (Directive (EU) 2015/2366) (PSD 2), 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. In accordance with these provisions, the Association was established on 17 September 2020. Accordingly, all payment and electronic money institutions are required to become members of the Association. The duties of the Association include, among other things, carrying out professional training, research and advertising activities, establishing standards for the industry and helping ensure coordination among members and with the regulator.

Finally, pursuant to the Economic Reforms Action Plan published by the Ministry of Treasury and Finance on 12 March 2021, A Fintech Strategy Document was prepared and published on 29 December 2021. One of the objectives of the National Fintech Strategy is the determination of a roadmap for drafting regulations that will support the development of the sector by establishing an authorised structure that will lead to the development of the financial technology field and ensure the necessary coordination and cooperation. Also, a finance and technology base will be established in the Istanbul Finance Center to support fintech startups.

FINANCIAL REGULATION

Regulatory bodies

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

The Legislative Proposal to Amend the Law on Payment and Security Settlement Systems, Payment Services, and Electronic Money Institutions and Other Laws (the Amending Law) was published in Official Gazette No. 30956, dated 22 November 2019, and entered into force on 1 January 2020. On the effective date of the Amending Law, the powers of the Banking Regulation and Supervision Agency (BRSA) set forth under the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions (Law No. 6493) were transferred to the Central Bank of the Republic of Turkey (CBRT). Accordingly, the CBRT has the authority to monitor legal relations to which the payment service providers are a party owing to their activities to determine issues and areas for development. The Amending Law also grants the CBRT the authority to determine the rules and procedures of the legal relations therein and form working committees if it deems the relevant activities harmful to the area of payments. Finally, 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 and the Communiqué on the Management and Supervision for Information Systems of the Payment E-Money Institutions.

In addition to the CBRT, the Turkish Financial Crimes Investigation (MASAK), which acts as Turkey's financial intelligence unit, effectively fights money laundering and terrorist financing (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). CMB's Communique on Principles on Investment Services and Activities and Ancillary Services No. III-37.1 and 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.

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?

A large number of financial services and activities are regulated in Turkey. Some of these activities, which trigger licensing, authorisation or registration requirements in Turkey, include, and are regulated by, the following.

- the CBRT authorises payment services, invoicing services, e-money services and system operator services;
- the Banking Regulatory and Supervisory Agency issues licences for banking and finance activities, such as banking services, factoring and financial leasing services;
- the Capital Market Authority 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;
- the Central Securities Depository of the Turkish Capital Markets provides its members with registration (public offering, etc), settlement and custody services;
- the Risk Center 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 to financial institutions that are members of the Risk Center.

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.

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 bank and credit institutions, which do not include payment service or e-money institutions. In fact, 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. The banks and credit institutions must be established and authorised by the Banking Regulation and Supervision Agency. 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. The agreement does not have to be in writing. However, security providers for these debts should provide their consent in written form as well. 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 DIBS 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. Law No. 7222 on the Amendment of Banking Law and Some Other Laws (the Amending Law), which was published in Official Gazette No. 31050, dated 25 February 2020, coming into force on the same date, introduced the concept of crowd-lending by an 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, the CMB is empowered to make determinations regarding crowdfunding activities that collect money from the public based on partnership or lending; hence, establishing the legal basis of the lending-based crowdfunding model. As per the Amending Law, the provisions of the banking legislation shall not be applied for the financing provided through lending-based crowdfunding and shall not be considered as deposit or participation fund acceptance. Regulations regarding lending-based crowdfunding affect the situation of the trading of the funds in the secondary market, which will be provided through a lending-based crowdfunding platform. The investment limits in debt-based crowdfunding are regulated in the Crowdfunding Communiqué (III – 35/A.2) published in Official Gazette No. 31641, dated 27 October 2021. In addition, within the scope of the Communiqué, it is regulated that secondary market transactions regarding funded company shares and debt instruments approved by the BIST can be carried out in the relevant market within the framework of the procedures and principles prepared by the BIST and approved by the CMB. However, platforms, with the exception of widely authorised brokerage houses, cannot mediate secondary market transactions regarding shares or debt instruments.

Finally, according to the Economic Reforms Action Plan, crowdfunding applications based on equity and lending will be implemented quickly for innovative companies' access to financing.

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 mainly 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 Communiqué (III – 35/A.2) was issued by the CMB and was published in Official Gazette No. 31641, dated 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. The Amending Law, which was published in Official Gazette No. 31050, dated 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 may bring 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 was clarified and venture companies, whose shares are monitored and recorded, are now allowed to hold general assembly meetings electronically. According to the Economic Reforms Action Plan, crowdfunding applications based on equity and lending will be implemented quickly for innovative companies' access to finance.

Additionally, peer-to-peer lending is not currently regulated in a manner synonymous with the definition found under PSD 2. However, lending-based crowdfunding platforms, which can be considered peer-to-peer lending, have been regulated as mentioned.

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 CMB.

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.

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 the 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 PSD 2. Lending-based crowdfunding platforms, which can be considered peer-to-peer lending, have been regulated under the Capital Markets Law and Communiqué No. III-35/A.2 on Crowdfunding.

Crowdfunding

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

Reward-based crowdfunding platform activities are not regulated in Turkey. Donation-based crowdfunding platforms may be subject to certain regulations. Both reward- and donation-based crowdfunding platform activities have been performed by several companies in Turkey.

In addition, equity and lending-based crowdfunding platforms are highly regulated under the Capital Markets Law. Law No. 7222 on the Amending Law, which was published in Official Gazette No. 31050, dated 25 February 2020, entering into force on the same date, introduced the concept of crowd-lending by the inclusion made to Law No. 6362. The Communiqué on Equity Based Crowdfunding III-35/A.1 was issued by the CMB and was published in Official Gazette No. 30907, dated 3 October 2019. Communiqué No. III-35/A.2 on Crowdfunding entered into force upon its publication in the Official Gazette, dated 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. 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. The CMB requires all platforms to be licensed by the CMB. 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-size technology and production companies to raise funds from capital markets without publicly offering shares.

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 Official Gazette No. 31069, dated 15 March 2020. The effective date of the Regulation, which also refers to sharing via application programming interface (API), was determined as 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.

Additionally, the Regulation on the Operating Principles of Digital Banks and Service Model Banking has been published in Official Gazette No. 31704, dated 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 the 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. In addition, the procedures and principles regarding the status of competition-sensitive data in data sharing to be made pursuant to this Regulation are determined by the CBRT by taking the opinion of the Competition Authority.

In addition, 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 Official Gazette No. 31676, dated 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 was regulated.

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, unlike other countries, 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, was 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, dated 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 artificial intelligence until 2025, to determine the strategic priorities, goals, targets and measures in this field and to implement them. The strategy was designed around six strategic priorities, namely:

- training AI experts and increasing employment in the domain;
- supporting research, entrepreneurship and innovation;
- facilitating access to quality data and technical infrastructure;
- regulating to accelerate socioeconomic adaptation;
- strengthening international cooperation; and
- accelerating structural and labour transformation.

Within the scope of these strategic priorities, 24 objectives and 119 measures were determined.

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.

Credit references

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

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 the Law No. 5411. The Risk Centre was established within the Banks Association of Turkey (TBB) for the purpose of collecting 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 ensuring 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 Centre of the TBB and provides data collection and sharing services to the 187 financial institutions that are members of the Risk Centre.

CROSS-BORDER REGULATION

Passporting

17 | Can regulated activities be passported into your jurisdiction?

Undoubtedly, one of the most remarkable changes made by the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers, which was published in Official Gazette No. 31676, dated 1 December 2021, was the regulation of the cooperation of fintech companies with legal entities residing abroad. According to the Regulation, payment institutions and e-money institutions will be able to cooperate with legal entities residing abroad, which have obtained permission from the 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 headquarters 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, with the adoption of the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers, it has been 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.

Pursuant to the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers, requirements for applications for operation permits are now tightened by way of a two-stage evaluation and the application fees and licence fees have been increased.

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 Bank's 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.

CHANGE OF CONTROL

Notification and consent

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

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

21 | 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), dated 27 December 2020. The term has been defined as to also include foreign-based financial companies. The aforementioned definition has been stipulated to comply with the regulation on 'financial groups' for which new obligations have been imposed within the scope of article 5 of Law No. 5549. The article regulates that companies affiliated with the financial group may share information within the group regarding accounts and transactions with the recognition of the customer to ensure that specified measures are taken at the group level. Information-sharing cannot be avoided by putting forward the provisions in special laws.

Within the framework of the Regulation on the Amendment of the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism, which entered into force through Presidential Decision No. 3941, dated 30 April 2021, published in Official Gazette No. 31471, dated 1 May 2021, crypto-asset service providers have been specified among the 'obliged parties' stipulated under the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism (the Regulation).

MASAK's guide titled Main Principles for the Crypto Asset Service Providers Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism (the Guide) includes information on administrative and legal sanctions to be imposed in the case of failing to fulfil the obligations that crypto-asset service providers have as obliged parties under the Regulation. Accordingly, failing to fulfil the obligation of know your customer; the obligation of suspicious transaction reporting; and the obligation of regular reporting may result in administrative fines to be imposed by MASAK under Law No. 5549.

Guidance

22 | 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 'crypto-asset', the Guide refers to the Regulation Prohibiting Payments Through Crypto Assets, which was published in Official Gazette No. 31456, dated 16 April 2021, which entered into force on 30 April 2021. The Guide defines the activities of crypto-asset service providers as 'the

mediation regarding the trading of the cryptoassets through electronic transaction platforms'. In addition, following the crypto asset service providers being determined as obliged parties by the relevant legal regulation, the Suspicious Transaction Reporting Guide was published on the official site of MASAK on 8 April 2022, aiming to explain the rules to which crypto asset service providers are subject to regarding the obligations stipulated under the Law No. 5549 including reporting of suspicious transactions.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Transferring loans is possible and is done by entering into an agreement between the transferor, the transferee and the debtor. The agreement does not have to be in writing. However, security providers for these debts should provide their consent in written form as well. The Compulsory Use of Turkish Language Law No. 805, dated 10 April 1926, requires all agreements by Turkish parties to be made in Turkish.

Loan agreements or security agreements are not allowed to be entered into on peer-to-peer or marketplace lending platforms, which have not been regulated or allowed to run yet.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

There are no registration requirements with the authorities in Turkey for a transfer or assignment of loans to be effective. However, peer-to-peer or marketplace lending platforms have not been allowed to run yet.

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

The primary piece of legislation that governs asset-backed securities and the risk retention system and requirements that must be put in place is the Communiqué on Asset Backed Securities No. III-59.1. The originator must retain the risk.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

There are two distinct regulations regarding the duty of confidentiality:

- the Banking Law (Law No. 5411); and
- the Personal Data Protection Law (Law No. 6698), codified on 24 March 2016, which bars and sets limitations on the disclosure, processing and transfer of personal information (which also includes borrower information).

In relation to special purpose vehicles (SPVs) being utilised for securitisation confidentiality, with the Communiqué on Principles of Venture Capital and Private Equity Investment Companies (III-48.3) there are no limitations on using these entities, but the scope of their confidentiality duties is limited to the duty of confidentiality provisions found within the Turkish Commercial Code, the Turkish Criminal Code and any bilateral agreement barring disclosure that the SPV involved in the securitisation transaction may be a party to. Consequently, SPVs are not awarded any special status, and any applicable duties, including the duty of confidentiality, still remain intact.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 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 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, dated 20 August 2021. The roadmap for work in the field of artificial intelligence 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 artificial intelligence until 2025, to determine the strategic priorities, goals, targets and measures in this field and to implement them.

In addition, 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 has been prepared by taking into account the studies 'Guidelines on Artificial Intelligence and Data Protection of the Directorate General of Human Rights and Rule of Law' of the Council of Europe, 'Recommendation of the Council on Artificial Intelligence' of the Organisation for Economic Co-operation and Development, and 'Ethics Guidelines for Trustworthy AI' of the European Commission. The Guide, after stating the general recommendations, sets certain recommendations on the protection of personal data in artificial intelligence applications, carried out by developers, manufacturers, service providers and decision-makers in the field of artificial intelligence. The Guide recommends that special attention should be paid to:

- personal data privacy in a way that is consistent with national and international regulations;
- relevant academic institutions, neutral experts and organisations should collaborate within the design phase of human-rights-based ethical and socially oriented artificial intelligence application;
- 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 the PDP Legislation.

Last, The Regulation on the Structure and Activities of the Türkiye Health Data Research and Artificial Intelligence Applications Institution was published in the Official Gazette, dated 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 was regulated.

Distributed ledger technology

28 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. Therefore, they are not forbidden.

Cryptoassets

29 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 has been published by the Central Bank of the Republic of Turkey (CBRT) in Official Gazette No. 31456, dated 16 April 2021, entering into force on 30 April 2021. With the regulation, the definition of 'crypto-asset' was made for the first time in the current legislation.

The Regulation regulates the subjects below:

- 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.

With the Regulation, payment service providers (banks, electronic money and payment institutions, Posta ve Telgraf Teşkilatı AŞ) cannot develop business models in a way that cryptoassets will be used directly or indirectly in the provision of payment services and issuing electronic money, it is stipulated that it cannot provide a service regarding the business model mentioned. In addition, payment and electronic money institutions are prohibited from intermediating on platforms that provide trading, custody, transfer or issue services regarding cryptoassets or fund transfers to be made from these platforms.

The Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions (Law No. 6493), and its supplemental secondary legislation, regulates the market and the concepts such as e-money, digital wallets and digital currencies. 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. In addition, the Turkish Banking Regulation and Supervision Agency explicitly states within its public announcement No. 2013/32 that cryptoassets are not to be considered e-money.

The use of digital wallets is allowed, but there are no rules or regulations governing this tool.

Also, e-money, which is regulated under Law No. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, can only be issued by e-money institutions authorised by the CBRT.

Finally, the Financial Crimes Investigation Board published the guide titled the Main Principles for the Crypto Asset Service Providers Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism on 4 May 2021. The Guide provides detailed and instructive application-oriented information regarding the obligations that the crypto asset service providers have under the Regulation as obliged parties, namely:

- know your customer (especially the identification of natural persons and legal persons, identification in subsequent transactions and remote identification);
- suspicious transaction reporting;
- providing information and documents;
- regular reporting; and
- retaining and submission.

Token issuance

30 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, neither cryptocurrencies nor cryptoassets can benefit from these rules and regulations.

In the Announcement made pursuant to Capital Markets Board Decision No. 47/1102, dated 27 September 2018, it is stated that ICO processes may have similar aspects to crowdfunding and public offering activities, and if the situation is evaluated within the scope of each concrete activity and if it has a similar nature to crowdfunding, it may enter the regulatory framework of the Capital Markets Board. However, at this point, the definition of crowdfunding in the Capital Markets Law is remarkable. According to this definition, crowdfunding can only be done through crowdfunding platforms. Therefore, 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, dated 30 April 2021, and drafted by the CBRT, no ban was imposed on the trading of cryptocurrencies on exchange platforms.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 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 laws that regulate personal data processing activities (namely, collection, domestic and cross-border transfers, destruction and protection) 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 Communiqué on Information Systems of Payment and Electronic Money Institutions and Data Sharing Services in the Field of Payment Services Providers were published in the Official Gazette, dated 1 December 2021. The Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers 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. In accordance with the Communiqué, the institutions are obliged to inform 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.

With the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers, 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. In addition, 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.

Also, with Law No. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions, the Central Bank of the Republic of Turkey (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. In addition, the procedures and principles regarding the status of competition-sensitive data in data sharing to be made pursuant to this regulation are determined by the CBRT by taking the opinion of the Competition Authority.

Finally, the Regulation on the Sharing of Confidential Information, which was published in Official Gazette No. 31501, dated 4 June 2021, regulates the sharing and transfer of bank secrets and customer secrets, confidentiality obligation exceptions and the principles regarding the sharing of confidential information.

Cybersecurity

32 | 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. 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, dated 13 July 2014.

Finally, the Presidential Circular on Information and Communication Security Measures, which was published by the Presidency on 6 July 2019, 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

33 | 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 be performed within Turkey.

Within the scope of the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers published in Official Gazette No. 31676, dated 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 the activities other than payment service provision and electronic money issuance, from an external service provider.

Cloud computing

34 | 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 was published in Official Gazette No. 31706, dated 31 January 2022. The Regulation 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.

Finally, 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.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

35 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.

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 09 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; works or runs with a machine or device, or is connected to a machine or device, together with that device, machine or system can be patented. 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 the 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

36 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 the Industrial Property Law (Law No. 6769), unless otherwise agreed upon because of special contracts made between the parties (employer and employee) or the nature of 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 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

37 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 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

38 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 protected also 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 or whole retainer fee in addition to a disciplinary fine.

Additionally, pursuant to the Amendment to the Banking Law published in the Official Gazette, dated 25 February 2020, save for the mandatory provisions of the relevant legislation, client information has been specified as 'client 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 Official Gazette No. 31501, dated 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. Within the scope of article 73 of Law No. 5411, regulations were made regarding the confidentiality obligation, exceptions and definition of 'customer secret'. In the Regulation, all information regarding real and legal persons becoming bank customers is included in the scope of customer secret. With the Regulation, it has been mandatory for banks to establish an information-sharing committee. The committee will be responsible for coordinating the sharing of customer secret and bank secret information, taking into account the proportionality factor, and recording these evaluations by evaluating the appropriateness of sharing requests. Last, due to the nature of the transaction, it has been necessary to interact with a bank, payment service provider, payment, security settlement or messaging systems established in the country or abroad, and it is a mandatory element of the transaction to share customer secret information with parties in the country or abroad to complete the transaction. For transactions such as domestic or international fund transfer, international letter of credit, letter of guarantee, reference letter, initiating the transaction by the customer or entering an order by the customer through the distribution channels for electronic banking services has been regarded as the customer's request or instruction in terms of such shares.

Branding

39 | 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 intellectual property 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

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

According to Law No. 5846, authors whose intellectual property 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

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

Since 2018, the Turkish Competition Authority (TCA) has rendered decisions in favour as well as against fintech companies. Recently, the TCA made a series of decisions that may potentially affect the market structure and the nature of competition in payment systems. Essentially, those decisions are based on the re-evaluation of earlier granted exemptions for certain services of the Interbank Card Centre (BKM). In brief, the TCA found that the BKM's digital wallet, BKM Express, is not qualified for exemption as its restrictive effects on competition outweigh the benefits to general welfare, and the TCA ordered the BKM to stop BKM Express services no later than 30 June 2020.

There are significant duties levied upon financial institutions regarding the duty of confidentiality within the 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.

Last, on 8 December 2021, the Report on Financial Technologies in Payment Services (the Report) was published on the website of the Competition Authority. The Report has been prepared to emphasise the importance of making maximum use of the radical transformation in the financial sector in Turkey and to reveal the necessity of inter-institutional cooperation in this field and focuses 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.

TAX

Incentives

42 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 R&D 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, dated 3 February 2021. In parallel with the practice implemented in R&D 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 Official Gazette No. 31207, dated 8 August 2020 , from 8 August 2020, the rate of bank and insurance transactions tax (BITT) is applied as zero 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

43 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, which was published in the Official Gazette, dated 7 December 2019, becoming effective three months following its publication. 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 liras in local revenue will be subject to a digital service tax at a rate of 7.5 per cent.

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

44 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

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

A developing fintech industry exists in Turkey. With regard to the long-awaited regulation in the field of payment services, it is safe to say that the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers will enable institutions to be more effective against the banks in the market. As the operations of payment and electronic money institutions are regulated under this Regulation, this will pave the way for the consumer to trust these institutions. On the other hand, there are new obligations and stricter rules for the institutions to carry out their operations starting with the obtainment of operating permits. Likewise, 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 they offer under similar conditions with other commercial customers, business partners and other payment service providers with which they make transactions, if other payment service providers wish to use such services.

Moreover, the Regulation on the Operating Principles of Digital Banks and Service Model Banking entered into force and the sector has completely reshaped following this. The Regulation being another new regulation gives more elbow room to fintech players to operate independent of banks, and this enables them to offer innovative services in the financial services sector. In this regard, we believe that the diversity of products and services arising from the independent atmosphere will positively impact the consumers purchasing products and services from the market.

These developments are of great significance in terms of providing services and innovative products that benefit consumers in the competitive conditions of the existing structure, as well as paving the way for

new innovative initiatives in fintech ecosystems. However, it can be said that, specifically with cryptoassets, the legislation is coming from a place of distrust among regulators. Additionally, Turkey's cryptocurrency law is expected to be ready by the end of 2022.

Also, the decisions of the Judges and Prosecutors Council on the establishment of specialised courts for cybercrimes and financial crimes were published in November 2021. Regarding the establishment of specialised courts, we consider that the determination of areas requiring legal expertise and the establishment of specialised courts are remarkable steps leading to progress on the judicial reform and the Human Rights Action Plan.

Turkish Payment Services and Electronic Money Association (the Association) aims to consolidate the data coming from its members in 2022 and to announce the sector reports. For this, it is planned to implement the TÖDEB Data Transfer System and to share the sector data with the public for the first time in 2022. The Association also plans to carry out studies that will increase the interest of new generations in the sector by organising training programmes to contribute to the employment of qualified personnel in the sector.

In addition, the Istanbul Financial Center Law was approved by the Grand National Assembly of Turkey's Planning and Budget Committee on 8 June 2022, and the regulation is anticipated to be published in the coming months.

With the Economic Reform Package, the planned regulations regarding the fintech world are as follows:

- within the scope of increasing financial inclusivity, a fintech strategy document will be prepared in which a roadmap for making regulations that will support the development of the sector will be determined by establishing an authorised structure that will lead the development of the field of financial technology and ensure the necessary coordination and cooperation;
- fintech institutions operating in the field of payments will have access to payment systems and public databases operated by the Central Bank of the Republic of Turkey (CBRT);
- representation of payment and electronic money institutions at the Interbank Card Center will be provided. A regulation test area (sandbox) will be established in the field of payments, which will strengthen the Istanbul Finance Center to becoming a global centre in the field of fintech;
- a finance and technology base will be established in the Istanbul Finance Center to support fintech startups;
- the Risk Center, which includes all financial credit and risk data of Turkey, will be reorganised under the control of the CBRT;
- the CBRT will form the economic, technological and legal infrastructure of digital money; and
- a surveillance mechanism will be established for the protection of financial consumers, market integrity and strengthening of competition.

SRP Legal

Cigdem Ayozger Ongun
cigdem@srp-legal.com

Deniz Erkan
deniz.erkan@srp-legal.com

Sakayıklı Sokak No. 10
Levent 34330
Istanbul
Turkey
Tel: +90 212 4014401
www.srp-legal.com

United Arab Emirates

Raza Rizvi and Muneer Khan

Simmons & Simmons

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

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

There is a generally progressive and ambitious trend 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 has its own regulatory bodies, and all the various regulators across all three jurisdictions have identified fintech innovation (albeit with some differing 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.

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 joined the Global Financial Innovation Network (GFIN), to, among other objectives, assist with cross-border testing.

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. The UAE Blockchain Strategy 2021 aims to have 50 per cent of all government transactions on the blockchain network by 2021. In October 2016, the UAE cabinet launched Government Accelerators as a new mechanism to boost the achievement of the National Agenda to achieve Vision 2021. 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 AI with a mandate that will cross over into fintech innovation. In August 2018, it was announced that the DIFC courts has partnered with Smart Dubai to create the world's first Court of Blockchain.

In May 2021, 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. 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 has its 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 regulation and rules from the outset; rather, a customised set of rules will be applied, which will depend on the business model, technology deployed and 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.

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, Dubai Law No. 4/2022 Regulating Virtual Assets in the Emirate of Dubai (the Dubai Virtual Assets Law), creating the Dubai Virtual Assets Regulatory Authority (DVARA) was passed. DVARA is to regulate 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). 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).

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 (ie, 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:

- 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 following a merger between the two institutions in 2020. 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:

- promoting, offering or issuing cryptoassets in the UAE;
- providing crypto-asset 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.

Consumer lending

5 | Is consumer lending regulated in your jurisdiction?

Yes. Article 65 of the 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 ensure 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.

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.

Following public consultation, with effect from 31 August 2017, 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 independently 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 409 to 412 of the Penal Code and is void under articles 204 and 714 of the Civil Code, interest is permitted under articles 77 and 90 of the Commercial Code, provided it does not exceed 12 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.

The DFSA issued a consultation paper in early 2017 called 'Crowdfunding: SME Financing through Lending', which proposed a regulatory framework to operate loan-based crowdfunding platforms in the DIFC. In summary, the DFSA proposed a regime whereby loan-based crowdfunding platforms in the DIFC:

- benefit from a new financial activity and licence for operating such a platform;
- apply appropriate prudential and conduct of business requirements for these platforms;
- disseminate appropriate risk warnings and disclosures to lenders and borrowers;

- conduct suitable due diligence on the borrowers as well as checks on lenders;
- deploy a business cessation plan in the event that it ceases operations; and
- follow rules in relation to transfer of rights and obligations between lenders.

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 (PFPs) serving equity investment, debt financing and trade receivables funding needs of start-ups, private enterprises and 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.

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.

On 10 September 2018, the FSRA 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.

In October 2020, the UAE Central Bank published Circular No. 7 of 2020 Loan-Based Crowd Funding Activities Regulations to introduce a framework for licensing, regulating and monitoring load-based crowdfunding platforms (CFPs), safeguard the financial system from the risks posed by such platforms, assist 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 had published its Regulatory Framework for Stored Values and Electronic Payment Systems, which covered digital payment services. This has since been replaced by the UAE Central Bank's Stored Value Facilities Regulation (the SVF Regulation), issued on 30 September 2020. In addition, the UAE Central Bank issued the Retail Payment Systems Regulation (the RPS Regulation) and 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 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.

Following the publication of the DFSA's Consultation Paper No. 125 on Proposals for Money Services in November 2019, the DFSA Rulebook COB Module has been amended, with effect from 1 April 2020, to introduce requirements for the provision of money services in relation to electronic money in the DIFC.

The FSRA has issued enhancements to its Regulations and Rules concerning Providing Money Services (PMS) in November 2020. The improvements includes 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.

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 379 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.

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 will be regulated by the UAE Central Bank following the merger between the Insurance Authority and the Central Bank under Federal Decree Law No. 25 of 2020. Under the law, the UAE Central Bank will assume regulatory, supervisory, licensing and enforcement functions for the insurance sector. On completion of the merger, the UAE Central Bank will ensure the implementation of best practices and standards in executing its mandate to supervise and regulate 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?

On 15 April 2018, the SCA issued Chairman of the SCA Board of Directors' Decision No. 18/RM of 2018 Concerning the Regulations as to Licensing Credit Rating Agencies. Under these regulations, 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 (ESCA), Financial Services Regulatory Authority (FSRA) and 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 significantly 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 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 true cross-border basis (ie, 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, Securities and Commodities Authority, DFSA or 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 (ADGM) 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 ADGM, and in many cases corresponding exemptions relating to these promotions, all of which differ according to the type of product or service offered.

CHANGE OF CONTROL

Notification and consent

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

Under the DIFC and ADGM frameworks, there are detailed provisions relating to changes of control, including where notifications need to be made with the DFSA or the FSRA 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 (SCA). Although the Insurance Authority and the UAE Central Bank have merged, 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.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

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

In March 2021, the SCA introduced the Board of Directors Decision No. 23/R.M 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 AML risks for Virtual Assets and Virtual Asset Services Providers, in addition to any standards issued by the UAE Central Bank in respect of FATF guidance. The SCA's regulations on virtual assets, that 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 Central Bank of the United Arab Emirates 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. However, the 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 crypto-asset 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 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 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 in order 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 ADGM. The ADGM's AML rules are contained in the Anti-Money Laundering and Sanctions Rules and Guidance Module to the FSRA 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 is able to provide an appropriate audit of trail of a transaction, 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.

Guidance

22 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.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

If any security is based within the UAE, the agreements should be entered into with a local security agent whereby the local security agent holds security on behalf of the service provider. Security may need to be perfected, depending on the type of asset to which the security relates.

In the Dubai International Financial Centre (DIFC), there is no licensing or registration requirement for a lender to take security over DIFC-based assets. Any real estate mortgages must be registered with the DIFC Register of Real Property without delay. For all other types of security interest, a security interest will be considered perfected if it has 'attached' and a financing statement has been filed with the DIFC Security Register. For security to 'attach', different procedures will need to be taken depending on the type of security interest under either the DIFC Real Property Law or the DIFC Law of Security (land, shares in a DIFC company, bank accounts, receivables, insurance, floating charges, etc). Similar protection requirements exist within the Abu Dhabi Global Market (ADGM).

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

In onshore UAE, an assignment of rights requires only notification from the assignor to the counterparty, confirming the assignment to the assignee. Where this is not possible, the bank may require this income to be deposited into a collection account, which will be covered by an accounts pledge.

In the DIFC, an assignment is perfected when it attaches (ie, when it becomes enforceable against the debtor or third party). The position in the ADGM is similar.

Assuming there are no contractual restrictions on transfers, the position in each of the relevant jurisdictions is as follows.

Onshore UAE

Article 1109 of the UAE Civil Code (Federal Law No. 5 of 1985) provides that the assignor, the assignee and the borrower must consent for there to be a valid assignment. There are Federal Supreme Court judgments holding that, in commercial matters, the consent to the assignment by the borrower is not necessary, although evidence will be required that the borrower has been notified of the assignment.

UAE law does not generally recognise the concept of beneficial ownership. Accordingly, an assignee of certain rights otherwise than in accordance with the UAE will not be recognised as having a beneficial interest in the rights to be assigned.

DIFC

The DIFC makes a distinction between assignment of rights and assignment of obligations. The DIFC Contract Law No. 6 of 2004 (the DIFC Contract Law) sets out several limitations on assignments and delegations. Under section 94 of the DIFC Contract Law, a contractual right can be assigned unless the substitution of a right of the assignee for the right of the assignor would:

- materially change the duty of the borrower;
- materially increase the burden or risk imposed on the borrower by his or her contract;
- materially impair the borrower's chance of obtaining return performance; or
- materially reduce its value to the obligor.

A contractual obligation can be transferred unless the obligee has a substantial interest in having the obligor perform or control the acts promised.

While there are no explicit requirements under the DIFC Contract Law to notify borrowers of an assignment or transfer, it is advisable that the borrower be notified of this assignment or transfer.

ADGM

In the ADGM, as per the ADGM Application of English Law Regulations 2015, the principles of English law relating to the assignment of rights and transfer of obligations would apply. Under English law, an assignment is perfected once notice is given to the borrower. In the absence of such notice, the assignee's rights under the assignment become an equitable right. The transfer of an obligation would require the consent of the borrower.

Borrower consent may be required prior to any assignment of loans.

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

There are currently no risk retention requirements within the onshore UAE legislation or the legislation of the DIFC or ADGM. However, while not imposed by UAE law, securitisations originating in the UAE may still be subject to risk retention rules depending on the relevant investor base that is being marketed to.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

There are likely to be contractual duties of confidentiality in the relevant local documentation that may require borrower consent prior to disclosure concerning the loans or the borrowers. Further, if the borrowers are data subjects for the purposes of the DIFC Data Protection Law or

the ADGM Data Protection Law, the special purpose vehicle may be treated as a processor for the purposes of those laws.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 | 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.

Otherwise, there are currently no rules or regulations governing the use of artificial intelligence or automated investment advice (ie, robo-advisory services) in the Dubai International Financial Centre (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).

Distributed ledger technology

28 | 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.

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, which aims to transform government transactions into the blockchain platform by the end of 2021.

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 DIFC. The Dubai Virtual Assets Regulatory Authority (DVARA) will be responsible for issuing permits for the provision of any virtual asset platform operation and management services.

As a result of the DFSA issued Consultation Paper No. 138 on the Regulation of Security Tokens, the DFSA launched a regulatory framework for investment tokens 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
- a cryptographically secured digital representation of rights and obligations that is issued, transferred and stored using DLT or other similar technology and: (1) confers rights and obligations that are substantially similar in nature to those conferred by a security or derivative; or (2) 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.

Cryptoassets

29 | 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 SCA Regulations.

The SCA issued Board of Directors Decision No. 23/R.M 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 DVARA, operate in Dubai and have a trade licence from the relevant commercial authority in Dubai. Applicants are currently granted an initial minimum viable product (MVP) licence by DVARA, which allows them to provide products and services to select groups of investors, before they are fully authorised.

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)) 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 March 2022 the DFSA published Consultation Paper No. 143 on the Regulation of Crypto Tokens (CP143). In this paper, the DFSA sought comment on its proposed regulatory framework for financial services activities in relation to crypto tokens. The regime proposed by CP143 seeks to complement the existing regulatory framework established in the DIFC, while simultaneously ensuring that the DFSA's approach remains relevant as technologies continue to develop. As a result, CP143 is very comprehensive, covering not only the definition and promotion of crypto tokens but also other regulatory requirements such as market abuse, Islamic finance and token custody. The deadline for responses was 8 May 2022 and the DFSA's new regulations are expected in either Q3 or Q4 of this year.

Token issuance

30 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, on 25 June 2018 the ADGM FSRA issued its framework for the regulation of spot crypto-asset 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 'crypto-asset 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 crypto-asset 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 crypto-asset that results in a fork (coding change), and the associated governance and control expectations for crypto-asset 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 crypto-asset 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 FRSA updated its virtual asset regulatory framework in February 2020.

Among other things, the key amendments included:

- changing the definition of 'crypto-asset' to 'virtual asset' (to align the terminology in the legalisation 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 mulitlateral trading facility and dealing in investments). This is to be 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/R.M 2020, which applies to exchanges based on cryptoassets.

In June 2021, the UAE Central Bank issued the RPSCS Regulation. This regulates payment service providers and requires firms providing payment token services in Onshore UAE (excluding the DIFC and 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 DVARA to provide services of exchange (ie, exchange between virtual assets and fiat currencies or between one or more form of virtual assets) and services relating to the offering of or trading in virtual tokens. While DVARA 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.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 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.

The Abu Dhabi Global Market (ADGM) and 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.

On 11 February 2021, the ADGM enacted the Data Protection Regulations 2021, which will replace the current Data Protection Regulations 2015. The regulations 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. The Data Protection Regulations of 2015 will continue to apply until the end of a transition period, starting from 14 February 2021, of 12 months for current establishments and six months for new establishments.

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 SVF Regulations require 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 require licences to implement an information retention and disposal policy to limit the data storage amount and retention time. In addition, 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 (ie, data is to be used and stored for the duration necessary to provide financial services).

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 the UAE PDP Law becoming enforceable), has the result that there is 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 be 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

32 | 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 Rumors 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.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

33 | 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 Central Bank of the United Arab Emirates 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 risks 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 share outside the UAE without the UAE Central Bank's approval and consent of their customers.

Cloud computing

34 | 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 outsourcings, which includes those within the financial services industry.

Organisations carrying out functions that are regulated by the Dubai Financial Services Authority (in the Dubai International Financial Centre)

or the Financial Services Regulatory Authority (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 apply 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.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

35 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

36 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 & 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 which 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 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

37 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

38 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 around 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

39 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 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 use of the proposed mark.

Remedies for infringement of IP

40 | 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

41 | 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 are 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

42 | 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 Abu Dhabi Global Market are all currently low or zero-tax jurisdictions.

Increased tax burden

43 | 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.

simmons+simmons

Raza Rizvi
raza.rizvi@simmons-simmons.com

Muneer Khan
muneer.khan@simmons-simmons.com

Office 17-04, Level 17
ICD Brookfield Place
Mustaqbal Street
Dubai International Financial Centre
Dubai
Tel: +971 4 709 6600
Fax: +971 4 709 6601
www.simmons-simmons.com

IMMIGRATION

Sector-specific schemes

44 | 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, 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 talents and expertise from all over the world.

UPDATE AND TRENDS

Current developments

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

No updates at this time.

United Kingdom

Angus McLean, Oliver Irons, David Trapp, George Morris, Jo Crookshank, Kate Cofman, Minesh Tanna and Olly Jones*

Simmons & Simmons

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.

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 2021.

According to data from the UK's fintech trade association, Innovate Finance, in 2021 fintech companies in the United Kingdom attracted US$11.6 billion in investment capital. That represented a 217 per cent increase from 2020 and meant that in 2021, the UK fintech sector attracted more investment than France, Germany, Sweden and the Netherlands combined.

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 2022 by the Economic Secretary to the Treasury, John Glen MP. In his speech to the Innovate Finance Global Summit during UK Fintech Week, Glen restated the government's desire to make the United Kingdom a pro-innovation jurisdiction, which is attractive to inward investment, and to fintech firms that do not have a settled base. For the first time, Glen also outlined the government's interest in fostering a supportive environment for cryptoasset businesses, saying that the government wants to make the United Kingdom 'the very best place in the world to start and scale crypto-companies'. It remains to be seen whether the new legislation being proposed by the government in relation to the regulation of cryptoasset businesses and the approach of the UK regulators in applying those regulations is consistent with these policy statements.

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. Currently, Project Innovate includes six initiatives:

- the Regulatory Sandbox 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;
- Innovation Pathways 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;

- Tech Challenges that are 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;
- TechSprints, also known as 'hackathons', are events that allow the FCA to gather participants from across the financial services industry and beyond to develop technology-based ideas and discuss specific industry challenges. The most recent TechSprint was the Crypto Sprint in May 2022, which was aimed at promoting new solutions and discussing regulatory concerns in the cryptoasset industry. Previous TechSprints have covered diverse topics from model-driven machine executable regulatory reporting to women's economic empowerment; and
- Showcase Days for regtech firms to demonstrate their technology solutions to internal market experts within the FCA.

Fintech and regtech firms that would like to participate in any of these initiatives need to apply to the FCA via the FCA Innovation Hub pages on the FCA's website at www.fca.org.uk/firms/innovation.

The FCA is also the founder member and chair of the Global Financial Innovation Network (GFIN). Formed in 2019, 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. 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 AI innovation between the public and private sectors. The BoE has also announced that it intends to work with the FCA to launch a 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 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.

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.

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':
  - securities include shares, bonds, debentures, government securities, warrants, units in a collective investment scheme (CIS) and rights under stakeholder and personal pension schemes;
  - contractually based investments include rights under certain insurance contracts (excluding contracts of general insurance), options, futures, contracts for differences and funeral plan contracts; and
  - relevant investments include the same investments as contractually based investments but also include contracts of general insurance;
- arranging deals in investments (this is split into two activities and specified investments in respect of arranging include securities and relevant investments):
  - arranging (bringing about) deals in investments, which applies to arrangements that have the direct effect of bringing about a deal; and
  - making arrangements with a view to transactions in investments, which is much wider and includes arrangements that facilitate others entering into transactions;
- 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 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
- electronic money: issuing electronic 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).

Consumer Duty

Consumer Duty is a new regulatory requirement, driven and regulated by the FCA, due to be implemented, 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 will require firms to review all UK products, services and communications aimed at retail customers. Firms will also 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.

The proposed implementation period gives firms until 30 April 2023 to implement this Duty.

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 and, potentially, certain forms of short-term interest-free credit under the RAO. HMT has also proposed amending the running-account exemption of section 60F(3) of the Financial Services and Markets Act 2000 (FSMA). Legislation is expected in mid-2023.

The government has also proposed reforming the CCA following the recommendations of the FCA's retained provisions report and the Woolard Review. Current proposals include bringing some of the substantive elements of the CCA into the direct remit of the FCA. Further details are expected.

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.

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:
  - in the case of credit provided to an individual, as or in connection with a dwelling by the borrower; or
  - in the case of credit provided to a trustee that is not an individual, as or in connection with a dwelling by an individual who is a beneficiary of the trust, or by a related person.

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 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 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 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.

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 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'; or
  - 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.

In January 2022, the FCA consulted on strengthening financial promotion rules for high-risk investments. One of the proposed changes would be to categorise P2P lending as a 'restricted mass-market investment', however, there are no changes proposed to the current restrictions on financial promotions in relation to P2P investments to retail customers.

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.

There is also a possibility that the firm may need to register with the FCA as an Annex 1 financial institution because it carries on commercial lending. As an Annex 1 financial institution, the firm would need to comply with all the detailed anti-money laundering requirements under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

Payment services

12 | Are payment services regulated in your jurisdiction?

Payment services are regulated under the PSRs, which implement the 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;
- 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;
- 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 PSRs 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'. 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 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. There have been no similar proposals from UK regulators, but such changes may influence the development of the PSR.

Key upcoming UK regulatory initiatives include proposals on bringing systemically important firms in payments chains under BoE regulation, creating rules and standards for Account to Account Payments, and the implementation of Confirmation of Payee services and other measures to tackle the rise in authorised push payment fraud.

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 PSRs require banks to allow third-party payment service providers to initiate payments from their customers' accounts.

In March 2022, the CMA provided an update on Open Banking and highlighted the following three items that required implementation:

- variable recurring payments for sweeping (due July 2022);
- enhanced management information submission mechanisms (due July 2022); and
- certain consent and access dashboard standards (due September 2022).

With regards to future regulations, HMT, the CMA, the FCA and PSR have issued a Joint Statement on the future of Open Banking, recommending a Joint Regulatory Oversight Committee to be led by the FCA and the PSR, which will agree and implement next steps.

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 (PRIIPs) 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.

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.

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 (MiFID II);
- 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.

The FCA is consulting on changes to strengthen the financial promotion rules for high-risk investments, with a Policy Statement expected in the summer of 2022. The FCA has proposed rationalising the classification of high-risk investments, introducing a package of measures to slow consumer journeys into high-risk investments, strengthening the role of firms approving financial promotions and applying the financial promotion rules to 'qualifying cryptoassets'.

A further HM Treasury consultation confirms that a 'regulatory gateway' for approving financial promotions will be introduced, whereby all new and existing authorised firms will be prohibited from approving the financial promotions of unauthorised persons, with a requirement to apply 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).

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;
- 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;
- 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

CHANGE OF CONTROL

Notification and consent

20 | 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 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 PRA can object to an application for a change of control.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

21 | 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 (MLRs) 2017. The United Kingdom implemented the Fifth Money Laundering Directive (5MLD) on 10 January 2020, by way of updates to the MLRs 2017 effected by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (the 2019 Regulations). Under 5MLD, and the 2019 Regulations (in line with the 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 (ICO) or initial exchange offering).

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.

HM Treasury (HMT) has updated the 2017 MLRs to exclude Account Information Service Providers from its scope.

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. 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.

HMT is consulting on proposed changes to the transfer of cryptoassets, and the 'travel rule' with the aim of bringing the United Kingdom in line with Financial Action Task Force Recommendation 16, regarding information sharing requirements for transferring cryptoassets. HMT is considering legislation that will require one of the originator's address, date, place of birth and passport number to be provided with a cross-border transfer of cryptoassets above €1,000.

Guidance

22 | 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 outline to its supervision of cryptoassets 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 issued a notice to all regulated firms reminding them of their existing obligations when interacting with or exposed to cryptoassets and related services (FCA Statement published 24 March 2022.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 | What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Provided the essential elements of a contract are present, loan agreements governed by English law can be executed in the form of agreements by signatories of the respective parties with due authority.

The execution requirements for an English law security agreement will depend on the form of security agreement. However, most English

law security agreements will be executed in the form of a deed to ensure that no challenge can be made on the grounds of a lack of consideration or owing to the form of property being secured. It is also common for a security agreement to grant the lender a power of attorney, which must be executed as a deed to be enforceable. Certain formalities are required for the execution of a deed:

- the deed must be in writing;
- it must be clear on its face that it is intended to take effect as a deed;
- it must be validly executed as a deed, the requirements of which will vary according to the executing party (eg, whether it is an individual or a company). In particular, if the executing party is a company and if the deed is signed by a director (rather than through the affixing of the company seal or the signature of two authorised signatories), the signature of such director must be attested by a witness (in other words, an individual must observe the execution of the deed and record, on the deed itself, that he or she has made such observation); and
- it must be delivered as a deed, which is to say that the parties must demonstrate an intention to be bound.

Typically, peer-to-peer (P2P) marketplace lending platforms require agreements to be entered into electronically (e-signing). The e-signing of simple contracts (such as loan agreements) is accepted as creating enforceable agreements, subject to complying with regulatory requirements (eg, in respect of regulated lending). E-signing can take a range of forms, including typing the signatory's name, signing through biodynamic software (ie, the signatory signing on a screen or on a digital pad) or clicking an 'I accept' (or similar) icon on a web page. Certain limitations on e-signing generally need to be borne in mind:

- English law prohibits e-signing in respect of certain types of contract, including but not limited to documents required to be registered at HM Land Registry;
- there may be restrictions within a company's articles of association that may restrict or forbid the use of e-signing, and these should be checked prior to any signing; and
- questions arise as to whether the prescribed formalities for executing deeds can be satisfied by e-signing. In particular, difficulties are likely to arise in satisfying the attestation requirement (where a deed is executed by an individual or by a single director of a company in the presence of a witness) by electronic means.

Even if it were possible to satisfy these formalities, there may be practical reasons (such as certainty and evidential issues) why executing a deed with a wet-ink signature (rather than e-signing it) may be preferable. As such, best practice remains for deeds to be executed with a wet-ink signature.

On 3 September 2019, the Law Commission published Law Com report No. 386 concerning e-signatures. Of particular importance, the Law Commission confirmed that e-signing is capable in law of being used to execute documents (including deeds), provided that:

- the executing party 'intends to authenticate' the document, which it clarified as the same as intending to be bound; and
- any formalities relating to the execution of such document are satisfied.

With respect to the attestation requirement, however, the Law Commission's views are that the physical presence of a witness is required, even when both the signatory and the witness are executing or attesting the document using e-signature. The Law Commission was not satisfied that the witness's 'virtual' or 'remote' presence would suffice, and this is also the position that is followed by the HM Land Registry. These views, and the law in respect of physical witness, remain unchanged since the beginning of the covid-19 pandemic.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

To perfect a legal assignment of loans originated on a P2P lending platform, various criteria must be met. Most importantly, notice of the assignment must be received by the other party to the loan agreement. In addition to this, the benefit under the loan that is being assigned must be absolute, unconditional and not purporting to be by way of charge only, the contract effecting the assignment of the loans must be in writing and signed by the assignor, and the assignment must be of the whole of the debt under the loan agreement.

Subject to certain exceptions, notice by email will comprise notice in writing under English law and, therefore, sending a notice to the other party to the loan agreement by email should not preclude it from being effectively delivered. However, a question remains over whether notice of assignment can be effectively delivered solely by updating the relevant party's account on the P2P lending platform. It is therefore best practice to notify the other party to the loan agreement of the assignment both by email and an update to their P2P account.

If the assignment does not comply with the above criteria for a legal assignment, it may nevertheless take effect as an equitable assignment. One of the key distinctions between a legal and an equitable assignment is that, in the case of an equitable assignment, the person to whom the loan has been transferred would not be able to bring an action under the contract in their own name.

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

Yes, the risk retention requirements set out in Regulation (EU) 2017/2402, as it forms part of the domestic law of the United Kingdom by virtue of the European Union (Withdrawal) Act 2018 (as amended by the European Union (Withdrawal Agreement) Act 2020), as amended by the Securitisation Regulations 2018 (SI 2018/1288) and by the Securitisation (Amendment) (EU Exit) Regulations 2019 (SI 2019/660) (referred to as the UK Securitisation Regulation) apply:

- directly to the 'originators', 'sponsors' and 'original lenders' of a 'securitisation' transaction (as each such term is defined in the UK Securitisation Regulation) where any of the originator, sponsor or original lender is established in the United Kingdom; and
- indirectly to originators, sponsors and original lenders of securitisation transactions that are offered to 'institutional investors' (as defined in the UK Securitisation Regulation) regulated by the Financial Conduct Authority (FCA) or Prudential Regulation Authority (PRA) (as it is incumbent upon institutional investors in securitisation transactions to ensure that the retention requirements under the UK Securitisation Regulation have been complied with).

If any party to a securitisation is established outside of the United Kingdom, or any investor is regulated by a competent authority other than the FCA or the PRA, it will also be necessary to consider the regulatory regimes in the other jurisdictions applicable to such party or investor. For example, if any securitisation is offered to an 'institutional investor' (as defined in the EU Securitisation Regulation) regulated by a competent authority of an EU member state, the risk retention requirements set out in Regulation (EU) 2017/2402 (the EU Securitisation Regulation) will apply indirectly to the originators, sponsors and original

lenders of that P2P securitisation (notwithstanding that each of them may be established in the United Kingdom, rather than the European Union), as the EU Securitisation Regulation also requires such investors to ensure that the retention requirements under the EU Securitisation Regulation have been complied with.

Each of the UK Securitisation Regulation and the EU Securitisation Regulation require the originator, sponsor or original lender in respect of a securitisation to retain on an ongoing basis a material net economic interest in such securitisation of not less than 5 per cent using one of five prescribed risk retention methods, including (among other things) retention of:

- the most subordinated tranches, so that the retention equals no less than 5 per cent of the nominal value of the securitised exposures;
- 5 per cent of the nominal value of each of the tranches sold to investors; or
- randomly selected exposures equivalent to no less than 5 per cent of the nominal value of the securitised exposures:
    - in the absence of agreement among the originator, sponsor or original lender as to who will be the retention holder, the originator shall be the retention holder;
    - originators, sponsors and original lenders may potentially be subject to a broad range of administrative sanctions (including significant fines) or remedial measures, or even criminal sanctions, where they have negligently or intentionally infringed the risk retention requirements. Investors in a securitisation that is non-compliant will be subject to higher regulatory capital charges; and
    - possible retaining entities in respect of a securitisation of loans originated on a P2P lending platform (a P2P securitisation)

Typically, a P2P lending platform will not qualify as the 'sponsor' or 'original lender' of a P2P securitisation. However, it may qualify as an 'originator' if it was (either itself or through related entities) directly or indirectly involved in the original agreement that created the P2P loans being securitised. Whether or not the P2P lending platform comprises an originator will ultimately be a question of fact, but it is likely that some P2P lending platforms in the market will (by virtue of their documentation structure and role as operator of the platform) comprise originators for the purposes of the UK Securitisation Regulation and (or) the EU Securitisation Regulation. If this is the case, any such P2P lending platform will be required to retain a 5 per cent economic interest in any securitisation of loans originated on their platform unless the originator, sponsor or original lender have agreed between them that another entity will retain.

If a P2P lending platform does either not qualify as an originator or does qualify as an originator but does not wish to retain, another entity with the capacity to retain will need to be identified and this entity will need to agree to retain in accordance with the terms of the UK Securitisation Regulation and (or) the EU Securitisation Regulation (as applicable). Any entity that retains in the capacity of 'originator' is expected to be an entity of substance, and each of the UK Securitisation Regulation and the EU Securitisation Regulation expressly provide that an entity will not be considered an originator where it has been established or operates for the sole purpose of securitising exposures. Neither the UK Securitisation Regulation nor the EU Securitisation Regulation specifies in what circumstances an entity will be considered to have been established for the sole purpose of securitising exposures and it is expected that this will be considered in secondary legislation taking the form of 'binding technical standards' (in the case of the UK Securitisation Regulation) or 'regulatory technical standards' (in the case of the EU Securitisation Regulation). At the time of writing, no binding technical standards or regulatory technical standards relating to risk retention have been adopted by the United Kingdom or the European Union (as applicable) or have come into force. However, in the Final Draft Regulatory Technical Standards relating to risk retention (published on 1 April 2022 pursuant to article 6(7) of the EU Securitisation Regulation), the European Banking Authority (EBA) proposed that an originator will not be considered to have been established with the 'sole purpose' of securitising exposures if it satisfies certain conditions, including that:

- it has a strategy and the capacity to meet payment obligations consistent with a broader business model that involves material support from capital, assets, fees or other sources of income, by virtue of which the entity does not rely on the exposures to be securitised, on any interests retained or proposed to be retained in accordance with the EU Securitisation Regulation or on any corresponding income from such exposures and interests as its sole or predominant source of revenue; and
- the responsible decision-makers have the necessary experience to enable the entity to pursue the established business strategy, as well as adequate corporate governance arrangements.

No equivalent draft binding technical standards have yet been published for review.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

The entity assigning loans to the special purpose vehicle (SPV) must ensure that there are no confidentiality requirements in the loan documents that would prevent it from disclosing information about the loans and the relevant borrowers to the SPV and the other securitisation parties. If there are such restrictions in the underlying loan documentation, the assignor will require the consent of the relevant borrower to disclose to the SPV and other securitisation parties the information they require before agreeing to the asset sale. In addition, the SPV will want to ensure that there are no restrictions in the loan documents that would prevent it from complying with its disclosure obligations under English and EU law (such as those set out in the EU Securitisation Regulation and the Capital Requirements Regulation).

Again, if such restrictions are included in the underlying loan documents, the SPV would be required to obtain the relevant borrower's consent to such disclosure. In addition, if the borrowers are individuals, the SPV, its agents and the P2P platform would each be required to comply with the statutory data protection requirements under English law.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 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 AI in the United Kingdom (including in respect of robo-advice). However, there are some limited regulatory provisions; most notably in the UK General Data Protection Regulation (UK GDPR) that set out requirements in respect of 'automated' decision-making (which would include AI and robo-advice) involving personal data. In particular, article 22 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, articles 13(2) and 14(2) require the data controller to provide 'meaningful information about the logic involved'. Fintech businesses using personal data in AI (eg, in assessing loan applications) will therefore need to be able to explain how the AI system operates in that context. The Information Commissioner's Office has released detailed guidance on compliance with data protection law when using AI (including the explainability provisions noted above) in its Guide to Data Protection and in its AI and Data Protection Risk Toolkit. The Information Commissioner's Office has also issued guidance specifically on explaining decisions made with AI in conjunction with the Alan Turing Institute.

The Final Report of the Financial Conduct Authority (FCA) and Bank of England's (BoE) Artificial Intelligence Public-Private Forum (AIPPF) published in February this year and two papers published by the FCA on AI in 2019 – 'Explaining why the computer says no' and 'Artificial Intelligence in the boardroom' – also 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).

Outside of this data privacy and explainability context, fintech businesses using AI (whether for robo-advice or otherwise) may still be subject to the FCA and (or) Prudential Regulatory Authority's (PRA) existing regulatory regimes. At the most general level, businesses must have regard to the high-level requirements of the FCA's Principles for Businesses and (or) PRA's 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. More specific regulation may also apply, for example, relating to individual accountability under the Senior Managers and Certification Regime or on operational resilience and outsourcing. Certain activities may also be subject to specific regulation, for example, investment advice provided by robo-advisers would be subject to conduct of business requirements, such as suitability assessments and disclosure of costs and charges, 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. One of the main purposes of the AIPPF was to identify such risks in financial services in the key areas of governance, data management, and model risk management and it set out in its Final Report examples of best practices of how to address and mitigate these risks. Building on the work of the AIPPF, the FCA and PRA will publish a Discussion Paper on AI later this year to address how existing regulation and legislation may be applied to AI.

In addition to the regulatory considerations detailed above, businesses using AI should also be aware of the National Security and Investment Act (NSI), which came into force on 4 January 2022. The NSI 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.

As the regulatory initiatives referenced above suggest, AI and its use by businesses is an issue attracting increased regulatory and governmental attention. Unsurprisingly, then, the law and regulation governing the use of AI is set to change. At the end of 2021, the government published its National AI Strategy, which included the commitment to publish later in 2022 a white paper setting out its position on the governance and regulation of AI. Meanwhile, 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.

Distributed ledger technology

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

Regulators in the United Kingdom in general seek to adopt a technology-neutral stance, regulating the outputs of systems rather than how they operate in the background. For example, the FCA in 2017 undertook a review of distributed ledger technology and its use in the financial services industry and concluded that no technology-specific regulation is required to govern its use. HM Treasury (HMT) has examined the potential role of distributed ledger technologies and has noted that:

> *existing financial services regulation and legislation were drafted without DLT in mind, meaning current legislative provisions may contain obstacles or ambiguities which hinder the adoption of DLT . . . The government intends to support industry in ensuring that legislation and regulation can accommodate tokenisation and DLT.*

A Financial Markets Infrastructure Sandbox is due to commence in 2023 which, in part, is aimed at giving the industry the opportunity to use distributed ledger technologies to provide financial markets infrastructure services (and be able to test in the market) with appropriate regulatory oversight.

However, some rules and regulations applicable in the United Kingdom indirectly have an effect on the deployment of distributed ledger technologies and blockchains as a result of the nature of the operation of these types of systems. For example, the GDPR generally requires personally identifiable information to be capable of erasure once it is no longer needed, which causes difficulties for those seeking to use distributed ledger technology to govern the use of that type of data, given the technology's generally 'immutable' (ie, unchangeable) nature. Another example is the Centralised Securities Depositary Regulation (an EU-level regulation applicable in the United Kingdom), which requires dematerialised securities to be settled through a centralised securities depositary, which is a hurdle to be overcome for those fintech businesses seeking to settle securities via distributed ledger technologies (security tokens).

Cryptoassets

29 | 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 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. These follow on from the FCA, BoE and HM Treasury's Crypto Assets Task Force report of 2018, which announced the intention to launch a series of consultations on regulation of the cryptoassets industry, including on:

- the transposition of the Fifth Anti-Money Laundering Directive into UK law (which resulted in the registration requirements mentioned earlier);
- guidance around the application of existing financial services regulation to the cryptoassets market;
- the potential extension of the FCA's regulatory perimeter to encompass certain assets and activities within the cryptoassets sector (which, as of the date of writing, has not yet been published); and
- a potential ban on the offering of derivative products to retail customers, where those products reference cryptoassets (which was published in 2019, and confirmed in 2020).

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 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 Regulator (PSRs); 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 characteristics with, and any businesses dealing in them need to be properly authorised by the FCA as appropriate.

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 registered under the PSRs for these payment services.

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 cryptoassets' (although this name is not yet confirmed), which would cover any:

> *cryptographically secured digital representation of monetary value which is, among other things stabilised by reference to one or more fiat currencies and/or is issued and used as a means of making payment transactions.*

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 FCA is, at the time of writing, consulting on these changes within the broader context of strengthening the financial promotion rules for high-risk investments.

The proposals include a broad definition of cryptoassets that would 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, certified sophisticated investors (a specifically defined class of investor), and high-net-worth companies would, however, be exempt. Common retail exemptions on the other hand would not apply, including promotions to high-net-worth individuals or sophisticated investors.

Together the proposals would mean significant restrictions on the promotion of cryptoassets – financial promotions in relation to these assets would, among other requirements, need to be fair, clear, and not misleading, include a prescribed risk warning, and be approved by a relevant FCA-authorised firm.

Crypto-asset 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

30 | 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), FSMA 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 financial promotion regime. This will include promotions in relation to the issuance of tokens

DATA PROTECTION AND CYBERSECURITY

Data protection

31 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 EU General Data Protection Regulation (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 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 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 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 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 whilst maintaining the UK's world-leading data protection standards'. We will have to wait and see the details of the bill once published, but there will be a difficult balance for the government to strike between creating something that provides the change that has been promised, while maintaining UK's adequacy status in the European Union and, in turn, the free-flow of personal data between the United Kingdom and European Union.

There are no rules or regulations in the United Kingdom relating to personal data that are specifically aimed at fintech companies.

Cybersecurity

32 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 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 Financial Conduct Authority (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

33 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 (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 Financial Conduct Authority (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 FCA have also published supervisory statements (Statements) that build on the Guidelines and set out the PRA and 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 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 are expected to comply with the expectations in the PRA Statement 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.

On 14 April 2021, the Bank of England 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 consultation closes on 14 July 2022 and the final guidance is likely to be published within the coming year.

Cloud computing

34 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

35 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 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

36 | 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

37 | 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

38 | 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 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

39 | 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

40 | 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

41 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 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 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), Financial Conduct Authority (FCA) and 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.

The CMA has been undertaking a number of initiatives to formulate its approach to the regulation of competition in the UK digital markets, with a view to focusing on the protection of the consumer. As well as undertaking an investigation into the retail banking market, seeking to implement open banking and 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. The CMA has been 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 'The CMA's Digital Markets Strategy: June 2019', which is a vision for how it proposes to protect consumers in complex and rapidly-changing digital markets while continuing to protect innovation.

One concrete outcome of this has been the creation of 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. In November 2020, the government announced the creation of a new unit, the Digital Markets Unit (DMU), housed in the CMA, which will focus on enforcing a new pro-competition regime covering online platforms with considerable market power.

The DMU was established within the CMA on 7 April 2021 to focus on operationalising and preparing for the new regulatory regime to be legislated.

On 9 March 2022, the government published its Plan for Digital Regulation, which aims to drive agile regulation, offering clarity and confidence to consumers and businesses. Regulation will be underpinned by three principles:

- actively promoting innovation,
- achieving forward-looking and coherent outcomes; and
- exploiting opportunities and addressing challenges in the international arena.

The Plan set out a timeline of strategy reviews and consultations that the government intended to undertake across three, six and 12 months including areas such as AI, cybersecurity, media literacy, innovation and national data.

In light of the above, there is proposed Digital Competition legislation that will soon be introduced to Parliament: the May 2022 Queen's Speech announced the government's plans to publish draft measures, and while this means a bill will not be introduced in the next parliamentary session (2022 to 2023), the government reconfirmed its intention to legislate as soon as parliamentary time allows. The intent of the legislation will be to designate firms that have strategic market status that will be subject to a mandatory code of conduct and pro-competitive interventions. This would formally also set up the DMU and set out its relevant powers and duties. Although it is operating to a degree since April 2021, its exact duties and the regime for which it will be monitoring compliance will be set out in the Digital Competition legislation.

The CMA has also taken an increasingly interventionist stance in UK merger cases. In part, this is probably a result of it having received more resources in preparation for Brexit; but also because of a growing feeling that it may have been missing transactions that have negatively impacted competition. This more interventionist approach has been present in all sectors to some extent, but it has been particularly noticeable in relation to fintech deals – a number of Phase II (in-depth) investigations have been related to transactions involving fintech players.

The future of fintech competition regulation will depend in some part on the UK's relationship with the EU post-Brexit. The FCA has as one of its priorities the development of future bilateral arrangements with the European Union and the rest of the world to promote its expertise in fintech regulation.

TAX

Incentives

42 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: an additional 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.

Subject to applicable lifetime limits, a company may raise up to £150,000 under the SEIS over a three-year investment period 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. 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.

In addition, in 2021 the government published a Call for Evidence on the Enterprise Management Incentive (EMI) scheme, which allows small and medium-sized enterprise to offer tax advantages on the exercise of qualifying share options offered to employees as a form of remuneration. Under the scheme, EMI options can be offered to individual employees up to a value of £250,000 per employee in a three-year period. The total market value of unexercised qualifying share options a company may grant under EMI cannot exceed £3 million. To qualify for the EMI scheme, a company must, at the relevant time, have less than £30 million in gross assets, fewer than 250 full-time employees and carry out a qualifying trade. In particular, the Call for Evidence will assess whether the government should expand the EMI scheme to support high-growth companies and how. Again, financial activities such as banking and insurance are excluded activities for the EMI scheme.

Following announcements made in the Autumn Budget 2021 and the 2022 Spring Statement, it is expected that from April 2023 qualifying expenditure for R&D tax relief will be expanded to include data and cloud costs and R&D supported by pure maths, though it will also be refocussed towards innovation carried out in the United Kingdom.

Increased tax burden

43 | 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 is due to increase 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.

From April 2022, the government introduced rules requiring large businesses to notify HM Revenue and Customs when they take a tax filing position in relation to VAT, corporation tax or income tax (including pay as you earn) that is uncertain, based on a number of triggers and subject to a de minimis of £5 million. The rules apply to businesses with a turnover above £200 million or a balance sheet totalling over £2 billion.

The government is also consulting in a number of other areas that may impact fintech businesses, including:

- how decentralised finance loans – where holders of cryptoassets lend them out for a return – are treated for tax purposes; and
- expanding the investment manager exemption to cryptoassets, using the proposed OECD definition as a starting point, thus enabling the exemption to cover not just cryptocurrencies, but targeting the definition at digital assets held by way of investments more generally.

IMMIGRATION

Sector-specific schemes

44 | 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, now need permission to work in the United Kingdom.

The Skilled Worker visa (formerly Tier 2) is most relevant. A candidate needs an offer from a licensed sponsor and the role must meet minimum skill and salary criteria. A lower salary may be paid where the worker is under 26, has a relevant PhD or science, technology, engineering and mathematics PhD or the role is a specified shortage occupation. IT business analysts, architects and system designers, programmers and software development professionals and cyber security specialists are currently shortage occupations but finance roles are not.

Licenced sponsors with linked overseas entities, may use the new Global Business Mobility (GBM) route, including the Senior and Specialist Worker category (formerly Tier 2 Intra-Company Transfer). 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 of 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 new route for those looking to set up a company in the United Kingdom. It can only be used by businesses that 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 a Start-Up visa subject to endorsement from a UK higher education institution or an organisation with a history of

supporting UK entrepreneurs. An Innovator visa is an option for those seeking to establish a new business in the United Kingdom with at least £50,000 of funds available for investment and subject to endorsement from a UK-authorised endorsing body. 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 by Tech Nation.

The new High Potential Individual visa, reminiscent of the Tier 1 (General) 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.

UPDATE AND TRENDS

Current developments

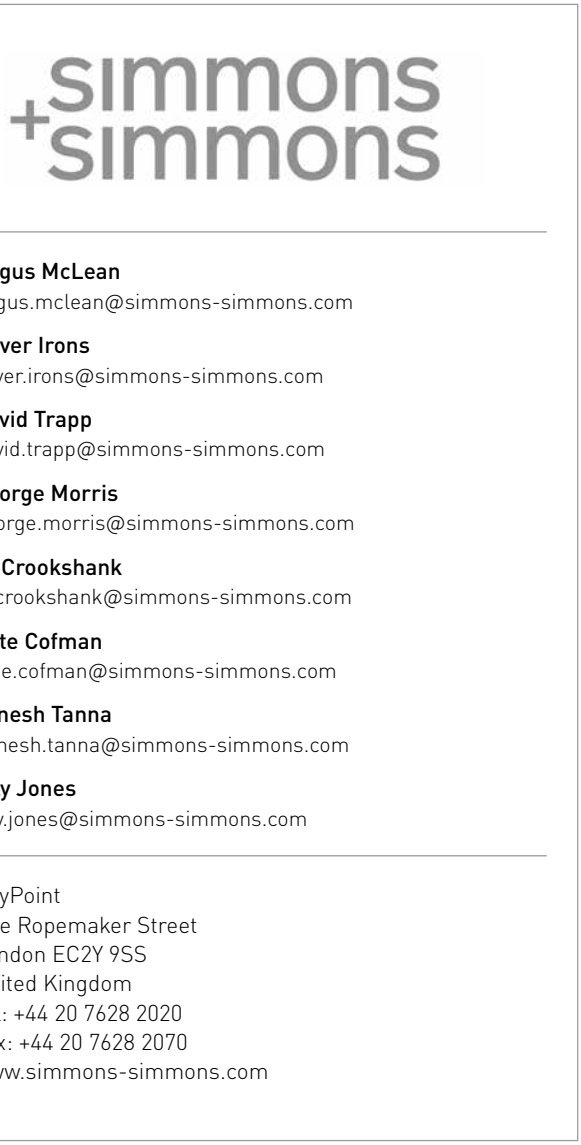
45 | Are there any other current developments or emerging trends to note?

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 and enforce new measures intended to encourage regulated firms to focus more on the impact of their activities on consumers (Consumer Duty).

In May 2022, The Financial Conduct Authority (FCA) and the Bank of England (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, FCA, BoE, Competition and Markets Authority and the Payment Services Regulator. Upcoming regulatory developments relevant to the fintech sector include:

- the coming into force of 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-advisors and insurers as well as payments, electronic money and crypto firms) in August 2022, with the deadline for compliance being April 2023 (subject to any extensions);
- publication of the policy statement clarifying how the government intends to implement its proposal to bring certain cryptoassets into the scope of financial promotions regulation;
- the implementation of the new legislation announced by the government in April 2022 to bring certain stablecoins (specifically payment cryptoassets) within the UK regulatory perimeter;
- further consultation by the BoE on the potential introduction of a UK central bank digital currency, building on the paper published by the BoE on 24 March 2022 with the responses it received to its Discussion Paper on new forms of digital money;
- the launch 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;
- an expected consultation on the proposed secondary legislation to bring buy-now-pay-later (or deferred) credit within the regulatory permitter. 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;
- a consultation on reforming the BoE's regulatory perimeter governing systemic payments firms;
- publication of a joint discussion paper by the FCA, BoE and the Prudential Regulation Authority on the oversight of Critical Third Parties (CTPs), which will inform future regulatory proposals relating to CTPs in technically complex areas, such as resilience testing;
- publication of a consultation paper on incident and outsourcing reporting arrangements;
- collaboration with the Information Commissioner's Office Innovation Hub (the innovation support programme led by the UK data privacy regulator, the Information Commissioner's Office) to provide bespoke data protection by design support for firms accepted into the FCA's Innovation Pathways function, and Regulatory Sandbox;
- a new survey on the use of machine learning in UK financial services (rerunning a 2019 survey); and
- publication of a joint discussion paper by the FCA and BoE on artificial intelligence building on the work of the Artificial Intelligence Public-Private Forum.

* *The authors wish to thank Sophie Sheldon, Angus Brown, Gordon Ritchie and Cherie Spinks of Simmons & Simmons LLP, and Gareth Wadley and Lizzie Field from Bristows LLP for their assistance in the preparation of this chapter.*



Angus McLean
angus.mclean@simmons-simmons.com

Oliver Irons
oliver.irons@simmons-simmons.com

David Trapp
david.trapp@simmons-simmons.com

George Morris
george.morris@simmons-simmons.com

Jo Crookshank
jo.crookshank@simmons-simmons.com

Kate Cofman
kate.cofman@simmons-simmons.com

Minesh Tanna
minesh.tanna@simmons-simmons.com

Olly Jones
olly.jones@simmons-simmons.com

CityPoint
One Ropemaker Street
London EC2Y 9SS
United Kingdom
Tel: +44 20 7628 2020
Fax: +44 20 7628 2070
www.simmons-simmons.com

United States

Paul T Clark, Jeffrey M Berman, Beth H Alter, Casey J Jennings and Jessica Cohn*
Seward & Kissel LLP

FINTECH LANDSCAPE AND INITIATIVES

General innovation climate

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

The United States has been a leader 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 pandemic, consumers increased their reliance on online and mobile financial services – a recent survey indicated 70 per cent of consumers now use mobile banking versus 57 per cent pre-pandemic. Mobile payment volume through PayPal increased 18 per cent in 2021, and 49 per cent through Zelle. 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. Volatility in the digital assets market in 2022 has spurred federal agencies as well as Congress to consider new regulation.

While 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, fintech firms have – thus far – been able to navigate existing banking and securities regulation without any material changes to the law. State and federal agencies have interpreted existing laws to extend their jurisdiction to protect consumers without stifling 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, Securities and Exchange Commission (SEC), and 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 (FINRA)	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?

Consumer lending is regulated at both the federal and state level.

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 (the SAFE 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 Advisors 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 Investment Advisers Act of 1940 (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 (ie, 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).

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 West Virginia and Iowa. Meanwhile, residents of Massachusetts, Mississippi, Nebraska and Nevada are ineligible for Payoff, another prominent 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 US, 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, which became effective on 21 June 2021, imposes disclosure requirements analogous to TILA, on providers of commercial financing in a principal amount of US$500,000 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.

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 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.

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.

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 (ie, property insurance, life insurance, etc).

Additionally, the majority of states have adopted some version of the Producer's 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.

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, for example, 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.

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 SEC broad discretion to deem securities marketing activities unlawful.

CHANGE OF CONTROL

Notification and consent

20 | 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 FINRA, must approve any change of control. For registered investment advisers, the Advisers Act 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.

FINANCIAL CRIME

Anti-bribery and anti-money laundering procedures

21 | 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. 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

22 | 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'.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Loan agreements and security agreements need to be properly authorised by the entity entering into the agreement and executed by an officer or authorised person who has the authority to sign the document on behalf of such entity. Subject to due authorisation, the requirements of the organisational documents of the signing entity and the requirement below, there are no particular requirements in the United States for executing these agreements.

Generally, there will not be any issue with the enforceability of loan agreements and security agreements entered into on a peer-to-peer or marketplace lending platform. Since these agreements will be executed electronically through an online platform, the requirements of applicable statutes relating to electronic signatures (including the Electronic Signatures and Records Act in New York, the Federal ESIGN Act, and the Uniform Electronic Transactions Act (UETA), which has been adopted by 49 states, all but New York) will apply. An electronic platform that requires a party to affirmatively consent to the documentation and preserves a record of such consent will likely satisfy the requirements of the applicable statute.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

To perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform, a UCC-1 financing statement must be filed in the applicable US jurisdictions naming the assignee as secured party and the assignor as debtor. If the assignment is not perfected by such a filing, the lack of perfection could result in the assignee being treated (1) as an unsecured creditor of the assignor rather than the owner of the assigned loans where the assignor files for bankruptcy in the US or (2) as having a lower priority interest in the loans where the assignor either unethically or accidentally sold the same loans to another party or another party claims to have purchased such loans or be a secured creditor with respect thereto and, in each case, such other party has filed a UCC-1 financing statement evidencing its interest in the loans.

It is possible to assign the loans without informing the borrower; however, until the borrower is notified of such assignment, the borrower would be able to discharge its obligations under the loan by paying the assignor. In such scenario, the assignee would only have recourse against the assignor for such amounts paid by the borrower.

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

Peer-to-peer or marketplace loan securitisations are subject to the risk retention requirements of section 15G of the Securities Act and Rule 15G thereunder, which require the person who organises a securitisation and sells assets to the issuing entity (ie, the sponsor of the securitisation) to retain 5 per cent of the credit risk associated with the securitisation. There are many factors that determine the sponsor of the securitisation and who is required to retain risk in compliance with section 15G and Rule 15G. The structure of the transaction, the holders of the loans being sold into the issuing entity and related financing structure can all impact the identity of the risk retention holder.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

The Gramm-Leach-Bliley Act (GLBA) governs the privacy and security of data processed and transferred by all financial institutions, including fintechs.

A 'financial institution' is defined, for the purposes of GLBA, as a business that is 'significantly engaged' in 'financial activities' as described in section 4(k) of the Bank Holding Company Act. The list of activities that have been deemed financial in nature is extensive and is likely broad enough to capture a special purpose company used to purchase and securitise peer-to-peer or marketplace loans.

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.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

27 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 and have applied their own definitions of the term. However, neither federal nor state level regulation of artificial intelligence 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 (SEC) as investment advisers.

Distributed ledger technology

28 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

cryptoassets. 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

29 | 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 crypto-asset is whether it constitutes a security. Traditional instruments such as notes, stocks, bonds and other instruments issued for capital raising purposes, including cryptoassets 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 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.

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 cryptoassets generally, or digital currencies specifically, has not yet materialised. A bi-partisan bill was recently 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. However, the bill is unlikely to become law in the near term.

Token issuance

30 | 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 recently suggested that 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. The SEC has recently approved new ATSs, and has proposed rules that would expand the reach of Regulation ATS.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 | 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. 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 US to another country. Consumer data may generally only be transferred from the EU 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, Virginia, and Utah, 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 GLBA.

Cybersecurity

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

GLBA is the primary federal law governing the security of data collected and processed by all financial institutions, including fintechs. 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.

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 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

33 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

34 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

35 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 protectible 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 in order 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

36 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: (1) the parties expressly agree in a signed written instrument that the work is a 'work made for hire', and (2) 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.

Joint ownership

37 | 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

38 | 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

39 | 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 US, 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

40 | 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 wilful 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 up to 10 years may be ordered.

COMPETITION

Sector-specific issues

41 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 APIs.)

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 Congress in the autumn of 2021 that highlighted its intention to pursue 'competition-based remedies' to consumer protection cases with regard to privacy.

TAX

Incentives

42 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

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

Under the Biden Administration's fiscal year 2022 budget proposals, a corporate income tax rate hike was proposed. It is unclear whether this rate hike will occur and how large an increase might be.

It is possible that the rules applicable to sales of 'qualified small business stock' may be limited if Congress amends this statute.

Although the United States has already enacted minimum corporate tax under the 'base erosion and anti-avoidance' tax, the United States may adopt new legislation that would impose a global minimum tax on certain corporations.

IMMIGRATION

Sector-specific schemes

44 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 oversees 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.
- 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

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

Multiple branches of the federal government are currently evaluating legislative or regulatory actions that could impact fintech firms and digital asset firms in the future.

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. Such a master account enables a holder to deposit funds into the account and draw cheques against it; earn interest on reserve bank balances held in the account; and have direct access to the Federal Reserve's Payment System Services without needing to partner with a regulated bank.

In April 2022, the Consumer Financial Protection Bureau (CFPB) announced that it would begin using a previously unexercised legal provision to examine nonbank financial companies that, in the opinion of the CFPB, pose risks to consumers.

New appointees to the Office of the Comptroller of the Currency (OCC), the CFPB and the Securities and Exchange Commission (SEC), 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.

With regard to digital assets, President Biden issued an Executive Order in March 2022 that laid out key principles for the development of a 'whole-of-government approach' to addressing risks specific to digital assets and encouraging responsible innovation. The Executive Order followed up on a November 2021 report of the President's Working Group on Financial Markets that focused on stablecoins, and recommended that they be issued by banks, to bring stablecoins under the 'umbrella' of federal banking regulation.

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. To that end, the SEC recently announced that it is hiring 20 enforcement attorneys in its Crypto Assets and Cyber Unit. The Federal Reserve has also been considering digital asset issues, publishing a discussion paper evaluating 'pros and cons' of a potential central bank digital currency in the United States. Additionally, Acting Chairman of the FDIC Martin Gruenberg called the need to 'evaluate crypto-asset risks' one of the FDIC's top four priorities for 2022.

There has also been legislation proposed relating to the regulation of digital assets. A bi-partisan bill was recently introduced in the Senate that would impose regulatory requirements on stablecoin issuers and transfer jurisdiction over most digital assets to the Commodity Futures Trading Commission. The bill is unlikely to become law in the near term. Moreover, the FDIC adopted a rule prohibiting misleading advertising and representations concerning the availability of FDIC insurance targeted at issuers of crypto 'stable coins.'

* *The authors acknowledge and appreciate the contributions of Jack Yoskowitz, Daniel Bresler, Daphne Coelho-Adam, Julia Spivack, Brett Cotler, and Joseph Nardello.*

SEWARD & KISSEL LLP

Paul T Clark
clark@sewkis.com

Jeffrey M Berman
bermanj@sewkis.com

Beth H Alter
alter@sewkis.com

Casey J Jennings
jennings@sewkis.com

Jessica Cohn
cohn@sewkis.com

901 K Street NW
Washington, DC 20001
United States
Tel: +1 202 737 8833
Fax: +1 212 480 8421

One Battery Park Plaza
New York, NY 10004
United States
Tel: +1 212 574 1200
Fax: +1 212 480 8421

www.sewkis.com

Vietnam

Le Thi Loc, Nguyen Duy Duong, Ta Nguyen Nhu Quynh and Ho Ngoc Quynh Anh*

YKVN

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; and 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 lending (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 unregulated segment, in practice some companies are operating in Vietnam by way of registering with the 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; and accordingly, recently, 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. In which, as assigned, the SBV is drafting a decree on the trial mechanism for controlling financial technology activities in the banking sector (sandbox) (the Fintech Draft Decree), listing seven fintech segments (the Seven Fintech Segments) that non-banking and finance companies (fintech companies) may be permitted to participate in the trial mechanism, including payment, credit, P2P lending, customer identification support, open application programming interface (Open API), innovative technology application solutions (eg, blockchain) and services to support banking activities (eg, credit scoring, savings and capital mobilisation).

In the near future, more developments are expected on the back of favourable regulations. Pending the regulatory sandbox of the SBV, fintech companies cannot engage in unregulated segments unless there is a special pilot approval of the PM.

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 (1) researching fintech activities, building, and developing legal framework for fintech; and (2) 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/QĐ-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 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 of 2020, with 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.

Accordingly, the SBV prepared the Fintech Draft Decree providing for the following two types of fintech companies participating in the Seven Fintech Segments: (1) fintech models and solutions not directly provided by banks; and (2) technology solutions applied or supported in banking activities. If the Fintech Draft Decree is adopted, fintech companies can engage in the Seven Fintech Segments, which are currently for banking and finance companies only.

In 2021, the PM issued Decision No. 316/QD-TTg approving pilot implementation of 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 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 current Fintech Draft Decree, the State Bank of Vietnam (SBV) is the sole regulator of fintech products and services, and it may seek opinions from different regulatory bodies for approving the sandbox for a specific fintech product or service, such as 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;
- 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 of 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 micro loans 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 (1) Law on Credit Institutions No. 47/2010/QH12, as amended from time to time (the Law on Credit Institutions); (2) Circular No. 39/2016/TT-NHNN prescribing lending transactions of credit institutions or foreign bank branches, or both, with customers (Circular 39); and (3) 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 (1) Vietnam-based commercial banks, foreign bank branches and foreign invested banks and (2) 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 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 agreement on amending the security conditions of the bad debt, a written approval of the borrower and guarantor must be obtained; and
  - the VAMC and credit institutions must report certain information to the SBV;
- trading in loans between persons being non-credit institutions or individuals is considered as assignment of rights to demand the payment of debts or assignment of obligation:
  - for assignment of right to demand, the transferer must provide a written notice to the obligor of such assignment, unless otherwise agreed; and
  - for assignment of obligation, the transferer must obtain a 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, and security investment companies and fund managers can receive funding or capital to carry out investment activities based on investment entrustment agreements.

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, and security investment companies and fund managers can receive funding or capital to carry out investment activities based on investment entrustment agreement. In particular, these investment activities are broadly

defined as (1) securities investment consultancy conducted by securities companies or securities investment fund managers, (2) securities investment fund management conducted by securities investment fund managers, (3) securities investment portfolio management conducted by securities investment fund managers, and (4) 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 (ie, 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 lending (P2P lending) is not regulated under the prevailing laws, and currently fintech companies are not allowed to engage in P2P lending. The SBV has expressed concerns over unregulated P2P lending companies applying exorbitant interest rates, high uninformed fees, or resort to threatening tactics, harassment and even violence to recover loans.

According to the Fintech Draft Decree, a P2P lending company can commence operation after complying with the following conditions: (1) being selected for the trial mechanism on P2P lending; (2) passing this trial mechanism for a certain period of time decided by the SBV and the PM; and (3) being subject to some restrictions on 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 application dossier to the SBV, who will review and examine it; if it is cleared by the SBV, it is submitted to the PM for approval 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 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: (1) being selected for the trial mechanism on crowdfunding; (2) passing this trial mechanism for a certain period of time decided by the SBV and the PM; and (3) being subject to some restrictions on 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 application dossier to the SBV, who will review and examine it; if it is cleared by the SBV, it is submitted to the PM for approval 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.

The government has assigned the SBV to draft the Fintech Draft Decree as a framework regulation on a trial mechanism in relation to an alternative financing solution for a borrower with cash flow problems with its investors to sell its unpaid or overdue invoices on e-commerce platform. Until the government adopts new regulations, the invoice trading is not allowed.

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 client's payment account; and
  - receipts and disbursements on behalf of others via client's payment account;
- 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 (CPTPP)). The competent authorities will decide on any limitations or technical barriers applicable to foreign investors who wish to engage in the IPS. 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 43 licensed IPS providers published on the SBV website; and
- the SBV is in process of amending existing regulations on non-cash payment (including the IPS). 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 the IPS are not

subject to SBV's licence requirement (ie, 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.

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 executive 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-advisors in Vietnam, except for securities segments.

In 2019, the PM 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 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 (ie, TCWealth).

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. However, it is currently unclear whether insurance products can be sold via an e-commerce platform operated by third parties. Thus, 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 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 MOF) before approving incorporation.

- For insurance agency services, in addition to incorporation documents, the company needs to meet the following requirements: execution of the insurance agency agreement with the insurer; and the staff being Vietnamese citizens, residing locally, at least 18 years old 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); conduct profitable business in three consecutive years prior to the application (for corporate investors holding more than 10 per cent of the charter capital); and undertake that their owner's equity less the minimum legal capital is at least equal to the planned amount of investment in insurance broker.

For (2) (advertising services), the display of the insurance products on platform (such as 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 WTO; 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 58/2021 (which takes effect on 15 August 2021), replacing Decree 10/2010. '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 pursuant to 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, minimum charter capital of 30 billion Vietnamese dong, and agreements with at least 15 participating institutions being Vietnam-based banks and foreign bank branches who 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 (1) international maritime transport and international commercial aviation and (2) 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 (1) entitled to provide payment services according to foreign law, including banks, international card organisations, switching organisations and payment intermediaries, etc; and (2) cooperating with a Vietnam-based bank or licensed IPS.

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 seven 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 MOF to sell its insurance products. In addition, the insurance companies must obtain the Ministry of Finance's (MOF) 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 provision of false information and false advertising of the scope of operation and insurance conditions, thereby causing damage to purchasers, is prohibited.

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 to 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. IPS providers can only provide the IPS pursuant to their IPS licence.

CHANGE OF CONTROL

Notification and consent

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

In 2017, the State Bank of Vietnam (SBV), through Official Letter No. 8104/NHNN-TT, requested all IPS providers to notify any change of their owners. The Non-cash Payment Draft, 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

21 | 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. Entities subject to the anti-money laundering regime must report certain transactions to it, including high-value transactions, suspicious transactions and transactions involving entities or individuals in the countries and territories on the 'blacklist' published by the Ministry of Public Security. Moreover, in addition to know-you-client procedures, entities subject to the anti-money laundering regime must perform 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

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

Payment transactions involving digital assets or cryptocurrency between the credit institutions are prohibited under current laws.

In 2018, the PM issued Directive No. 10/CT-TTg on 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, micro-finance institutions and people's credit funds) and IPS 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.

PEER-TO-PEER AND MARKETPLACE LENDING

Execution and enforceability of loan agreements

23 What are the requirements for executing loan agreements or security agreements? Is there a risk that loan agreements or security agreements entered into on a peer-to-peer or marketplace lending platform will not be enforceable?

Under the Law on Credit Institutions and Circular 39, execution of loan agreements and security agreements must satisfy certain conditions as follows:

- loan agreement must be made in writing and include the following compulsory contents, among others: the loan amount or credit line, the loan purpose, currencies for lending or repayment, the lending method, the lending term, interest, the rights and obligations of the borrower in providing documents and information in the assessment and decision on lending. Normally, bank loans must be made in writing and conducted physically at the banks to verify the borrower through checking the borrowers' documents, verifying conditions for borrowing and supporting documents, and deciding on lending. Recently, the State Bank of Vietnam (SBV) introduced electronic know-your-client procedures to verify customers for opening payment accounts, and this may lead to further opening in other banking products; and
- security arrangements for loans are subject to agreement between the lender and borrower; however, secured assets must be identifiable, owned by the securing party, not be prohibited from being traded or assigned, and not be subject to any disputes. If the collateral is real property, it must be notarised and recorded in title document.

As peer-to-peer (P2P) lending is a new business model in Vietnam where loan execution relies on the platform, the involved parties cannot identify the information and status of other side. Currently, there is no specific requirement on execution loan agreements and security agreements entered into on a P2P platform. In the authorities' view, the P2P platform does not sufficiently protect consumers.

Assignment of loans

24 What steps are required to perfect an assignment of loans originated on a peer-to-peer or marketplace lending platform? What are the implications for the purchaser if the assignment is not perfected? Is it possible to assign these loans without informing the borrower?

A P2P or marketplace lending platform is not yet recognised in Vietnam; thus, there is no legal framework on assignment of loan originated on a P2P or marketplace lending platform.

Securitisation risk retention requirements

25 Are securitisation transactions subject to risk retention requirements?

Securitisation is not regulated or recognised in Vietnam.

Securitisation confidentiality and data protection requirements

26 Is a special purpose company used to purchase and securitise peer-to-peer or marketplace loans subject to a duty of confidentiality or data protection laws regarding information relating to the borrowers?

Securitisation is not regulated or recognised in Vietnam.

ARTIFICIAL INTELLIGENCE, DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOASSETS

Artificial intelligence

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

In 2021, the 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 programmes. 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.

Distributed ledger technology

28 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 Vietnam is prohibited.

However, in 2021, the PM 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 in the Fintech Draft Decree.

Cryptoassets

29 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 IPS 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 'prepaid card'.

Token issuance

30 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.

DATA PROTECTION AND CYBERSECURITY

Data protection

31 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: it sets out the main requirements and principles on, among other things, data protection in the cyberspace to 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 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: it requires overseas and local companies that (1) are providing services on telecommunication networks, the internet and other value-added services in the cyberspace in Vietnam, (ie, cyberspace service providers); and (2) 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.

Certain authorities (eg, the Ministry of Public Security) are assisting the government in drafting a decree guiding the Law on Cybersecurity. Under the draft decrees on cybersecurity and personal data protection that have been open for public comment, there may be new requirements for data localisations, data protection officers and government approvals prior to cross-border transfers of personal data.

Cybersecurity

32 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 the cyberspace in Vietnam must be stored in Vietnam. In addition, this personal information of users must be protected.

In addition, the Law on Cybersecurity prohibits the use of the cyberspace (by anyone) to conduct the following acts:

- using the 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; or 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.

OUTSOURCING AND CLOUD COMPUTING

Outsourcing

33 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 State Bank of Vietnam's guidance. Credit institutions can lease technical infrastructure from third parties and must be responsible for performing e-transactions through these facilities, including preserving confidentiality of personal information and information of enterprises and organisations, ensuring security of information system, participating in response to incidents and taking remedial actions in accordance with the law.

Cloud computing

34 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 operation 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: (1) comply with the laws of Vietnam; and (2) have been granted a valid international certificate of information security.

INTELLECTUAL PROPERTY RIGHTS

IP protection for software

35 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 readable by a computer, are capable of enabling the computer to perform a job or achieve a specific result in accordance with Law on Intellectual Property No. 50/2005/QH11 as amended in 2009 and 2019 (the IP Law). Accordingly, 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 (ie, the right to give titles, the right to attach real name or pseudonyms, the right to publish or authorise to public and the right to protect the integrity) and economic rights (ie, the right to make derivative, display, reproduce, distribute, communicate and lease works). 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, language, whether it is published or unpublished or whether it is registered or unregistered.

IP developed by employees and contractors

36 | 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 are not necessarily the same. Under the IP Law, unless otherwise agreed, (1) 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 (2) for other industrial property right (ie, 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 as 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 (1) all the economic rights pertaining to this work and (2) only the moral right to publish his or her works or to authorise other persons to publish his or her works.

Joint ownership

37 | 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 the moral rights. Joint owners are not restricted from using, licensing, charging or assigning if both agree to do so.

Trade secrets

38 | 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: (1) it is neither common knowledge nor easily obtainable; (2) when used in business activities, it will create for its holder advantages over those who do not hold or use it; and (3) 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

39 | 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 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

40 | 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: (1) giving instructional information that the product is the subject of intellectual property rights and to warn others not to infringe; and (2) using means or technical measures to mark, identify, distinguish and protect the protected product;
- to request any infringing party to terminate such act, 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

41 | 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

42 | 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, and 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

43 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.

IMMIGRATION

Sector-specific schemes

44 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

45 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 IPS providers to build out their services.

* *The information in this chapter was accurate as at September 2021.*

Le Thi Loc
loc.le@ykvn-law.com

Nguyen Duy Duong
duong.nguyen@ykvn-law.com

Ta Nguyen Nhu Quynh
quynh.ta@ykvn-law.com

Ho Ngoc Quynh Anh
anh.ho@ykvn-law.com

Suite 1102
The Metropolitan
235 Dong Khoi Street
District 1
Ho Chi Minh City
Vietnam
Tel: +84 28 3822 31 55
www.ykvn-law.com

simmons+simmons

Our fintech team delivers legal and commercial advice for a wide range of businesses from fast-growing start-ups to some of the world's largest companies.

The Simmons team has been immersed in the fintech ecosystem since 2014 – a lifetime by the standards of this rapidly-evolving sector. We have extensive knowledge of the sector and an established network allowing us to support our clients beyond the realms of traditional legal advice.

Working with organisations across a broad range of verticals including crypto assets, payments, distributed ledger technology, digital banking, crowdfunding, wealthtech, insurtech and regtech – we help our clients address a wide range of legal challenges. For start-up and scale-up businesses we advise on regulation, tax, employment, incentives, IP, structuring, corporate governance and investment – supporting many towards unicorn status. For our global institutional clients, we advise on areas such as product development, commercial agreements, partnerships, investments and M&A.

Our understanding of the base technology underpinning fintech solutions combined with our knowledge of financial regulation sets us apart. It means our clients, regulators, and policy makers want to work closely with us. We have lawyers on the ground in key fintech hubs, including Hong Kong, Singapore, the UAE and the UK.

simmons-simmons.com

Other titles available in this series

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

Also available digitally

lexology.com/gtdt

ISBN 978-1-83862-539-9