Table of Contents

Section 1 General

1.1 Statement of Purpose

[Sample Client] designed these policies and procedures to safeguard its legal responsibility to comply with applicable residential lending laws and regulations. The board of directors and senior management, through a sound Compliance Management System, ensure the integration of these policies and procedures into the overall framework for product design, delivery and administration across the residential lending origination and service life cycle. Management and employees utilize these policies and procedures to guide their daily responsibilities to effect mitigation of regulatory compliance risk within their job roles.

1.2 Objective

The guidance in this guide applies throughout [Sample Client]'s operations with the objective to mitigate regulatory risk and consumer harm within the standards of [Sample Client]'s compliance program. [Sample Client] requires employees, contractors, and third-party vendors to comply with these policies and procedures.

1.3 State Law and Agency Guidelines

Federal law may alter, affect, or preempt state laws that are inconsistent with the federal law. Preemption applies only to the extent of the inconsistency. A state law is not inconsistent if it is more protective of a consumer. Wherever state law or local regulations overlap and provide greater consumer protections than federal law or the requirements set out in this guide, [Sample Client] will comply with the more protective law or regulation and will consult with the appropriate legal counsel to set forth [Sample Client]'s policies and procedures for compliance.

In some instances, agencies may overlay guidelines that expand upon the requirements of federal law. [Sample Client] must be cognizant of agency guidelines and incorporate those guidelines into [Sample Client]'s policies and procedures.

Section 2 Summary

The Currency and Foreign Transactions Reporting Act of 1970, commonly referred to as the Bank Secrecy Act (BSA), requires US financial institutions to assist federal government agencies in detecting and preventing money laundering.

The BSA is sometimes referred to as an anti-money laundering (AML) law or BSA/AML. Several acts, including provisions in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) and the Anti-Money Laundering Act (AMLA) amend the BSA.

The Bank Secrecy Act (BSA) establishes program, recordkeeping, and reporting requirements for national banks, federal savings associations, and federal branches and agencies of foreign banks.

The BSA and related anti-money laundering laws require the following of financial institutions:

- Establish effective BSA/AML compliance programs
- Establish effective customer due diligence systems and monitoring programs
- Screen against Office of Foreign Assets Control (OFAC) and other government lists
- Establish an effective suspicious activity monitoring and reporting process
- Develop risk-based anti-money laundering programs

In addition, amendments to the BSA incorporate the provisions of the USA PATRIOT Act which require a customer identification program. Office of Foreign Asset Control (OFAC) sanctions and Customer Identification Program (CIP) procedures must be part of a BSA/AML compliance program.

Section 3 Requirements

3.1 BSA Compliance Programs

Financial institutions must establish and maintain BSA/AML compliance programs consisting of procedures reasonably designed to assure and monitor compliance with BSA regulatory requirements. The BSA/AML compliance program must be written, approved by the board of directors, and noted in the board minutes. The BSA/AML compliance program must be commensurate with the bank's risk profile, as periodically updated, for money laundering, terrorist activity, and other illicit financial activity.

The BSA/AML compliance program must provide for the following:

- A system of internal controls to assure ongoing compliance
- Independent testing for compliance to be conducted by bank personnel or by an outside party
- One or more designated individuals responsible for coordinating and monitoring day-to-day compliance, such as a BSA/AML compliance officer
- Training for appropriate personnel
- A customer identification program (CIP) with risk-based procedures that enable forming a reasonable belief that the true identity of its customers is known
- Appropriate risk-based procedures for conducting ongoing customer due diligence (CDD) and complying with beneficial ownership requirements for legal entity customers

3.1.1 Board of Directors and Senior Management

The board of directors is ultimately responsible for BSA/AML compliance, including the designation of a qualified BSA/AML compliance officer. The board is responsible for providing oversight for senior management and the BSA/AML compliance officer in the implementation of a board-approved BSA/AML compliance program. The BSA/AML compliance officer must regularly report the status of ongoing compliance with the BSA to the board of directors and senior management so they can make informed decisions about existing risk exposure and the overall BSA/AML compliance program. Senior management and the board of directors are responsible for ensuring that the BSA/AML compliance officer has sufficient authority, independence, and resources—monetary, physical, and personnel—to administer an effective BSA/AML compliance program based on the institution's risk profile.

Section 4 Origination Compliance

The following are the primary roles of [Sample Client] origination in BSA/AML compliance:

- Comply with CIP information collection and validation processes to confirm the true identity of each customer and beneficial owner of legal entity customers and follow applicable procedures if identity verification cannot be completed on an individual
- Monitor for any customer appearing on any list of known or suspected terrorists or terrorist organizations alerts, such as the SDN list, and if an alert is present, ensure the loan is documented thoroughly to support the disposition of the alert which may include referring the file for review or filing of a SAR
- Provide the following required notices, as applicable:
  - Account Opening Notice
  - Certification of Beneficial Owners

4.1 Customer Identity Verification

[Sample Client] origination must apply customer identity verification procedures when a customer opens a new account to enable it to form a reasonable belief that it knows the true identify of each customer.

> The requirement does not apply to an existing customer as long as [Sample Client] has a reasonable belief that it knows the true identity of the customer.

[Sample Client] origination must obtain the applicable identifying information from each customer prior to opening an account either by using documents or through non-documentary means.

Refer to Customer Information Program in this guide for additional information.

4.1.1 Documentary Identification of Individuals

Before opening an account for an individual, [Sample Client] origination must obtain, at a minimum, the following identification information from the customer:

- Name
- Date of birth
- Address, which may be a residential or business street address, or if the individual does not have such an address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, the residential or business street address of next of kin or of another contact individual, or a description of the customer's physical location

Section 5 Servicing Compliance

The following are two primary roles of [Sample Client] servicing in BSA/AML compliance:

- Performing OFAC screening on certain loss mitigation activities and assumption transactions to identify any customer appearing on a list of known or suspected terrorists or terrorist organizations, such as the SDN list, and if an alert is present ensuring the loan is documented thoroughly to support the disposition of the alert which may include referring the file for review or filing of a SAR
- Sharing information with law enforcement if requested by FinCEN and participating in voluntary information sharing with other financial institutions, as applicable

5.1 Office of Foreign Asset Control Screening

[Sample Client] servicing must determine whether a customer for certain loss mitigation activities and assumption transactions appears on any list of known or suspected terrorists or terrorist organizations by checking the names of all persons subject to this requirement against current OFAC lists which may include, but are not limited to, the following:

- Treasury's OFAC Specifically Designated Nationals and Blocked Persons list
- Embargoed countries and regions list
- Other similar, renamed, or replacement lists

[Sample Client] must consult the list on the Department of the Treasury OFAC website regularly and subscribe or access the lists to receive updates as they occur. [Sample Client] must also review existing accounts against these lists as they are updated and document the review.

Refer to the OFAC sanctions lists on the Department of the Treasury website.

If [Sample Client] servicing determines that a customer, or someone with or for whom the customer is transacting, is on OFAC's Specially Designated Nationals (SDN) list or is from or engaging in transactions with a person or entity located in an embargoed country or region, [Sample Client] servicing must take the following actions:

- Notify the BSA/AML compliance officer to report the prohibited transaction to OFAC within ten business days of occurrence
- Reject the transaction

Refer to Office of Foreign Asset Control Screening Requirements in this guide for additional information.