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.

2.1 Coverage

Banks and nonbank residential mortgage lenders and originators (RMLOs) play important roles in helping regulatory agencies identify and take action against money-laundering entities.

The Financial Crimes Enforcement Network (FinCEN) is the administrator of the BSA. The Federal Financial Institutions Examination Council (FFIEC) is the interagency body empowered to prescribe uniform principles, standards, and report forms for the federal

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,

- 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
- If the customer is a US person, an employer identification number, or if the person does not have an employer identification number or is not required to apply for an employer identification number, the Social Security numbers of the principals involved with the account

[Sample Client] must verify the identity, account number, and Social Security or taxpayer identification number, if any, of any person or entity on whose behalf such transaction is to be effected by obtaining one or more of the documents acceptable as evidence of the true identity of the customer.

[Sample Client], based on its risk assessment, may require additional identifying information for certain customers or product lines.

4.1.2 Non-Documentary Identification

[Sample Client] origination may use any or all the following non-documentary methods of verifying identity:

- Contacting a customer
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, employer, or other source
- Checking references with financial institutions

[Sample Client] must use non-documentary methods of verification in the following situations:

- The customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard
- [Sample Client] staff is unfamiliar with the documents the customer presents for identification verification
- Other circumstances exist that increase the risk that [Sample Client] will be unable to verify the true identity of the customer through documentary means

[Sample Client] must verify the information within a reasonable time before a transaction is completed. Depending on the nature of the requested transaction, [Sample Client] may

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

5.1.1 Exception for Licensed Transactions

If a customer claims to have a license issued by OFAC permitting certain transactions that would otherwise be prohibited, [Sample Client] servicing must access the OFAC website to verify the license and that the transaction conforms to the terms and conditions of the license by taking the following actions as applicable:

- For a specific license, [Sample Client] must verify the transaction conforms to the terms and conditions of the license and must obtain and retain a copy of the authorizing license for recordkeeping purposes.
- For a general license, [Sample Client] must verify the transaction meets the relevant criteria of the general license before processing a transaction that may be covered under a general license.

5.2 Information Sharing

5.2.1 Information Sharing with Law Enforcement

If a law enforcement agency investigating terrorist activity or money laundering asks FinCEN to solicit, on its behalf, certain information from [Sample Client], FinCEN may require [Sample Client] to search its records to determine whether it maintains or has maintained accounts for, or has engaged in transactions with, any specified individual, entity, or organization.

[Sample Client] servicing must conduct a one-time search of its records to identify accounts or transactions of a named suspect. Unless otherwise instructed, [Sample Client] must search for current accounts, accounts maintained during the preceding 12 months, and transactions conducted outside of an account by or on behalf of a named suspect during the preceding six months. [Sample Client] must report any positive matches to FinCEN within 14 days, unless otherwise specified in the information request.

Refer to Information Sharing between Law Enforcement and Financial Institutions in this guide for additional information.