Table of Contents

1 BSA/AML Summary

_____(the institution) has adopted the following policies and procedures to comply with federal regulatory requirements pursuant to the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) laws. The institution shall establish and monitor compliance on a corporate-wide level and include all branches and service platforms. Compliance is applicable to all employees, agents, affiliates, third party brokers, loan correspondents, closing agents, and any other service providers.

The objective of this policy is to detect and report to the Financial Crimes Enforcement Network (FinCEN) any suspicious transaction or transactions involving a certain threshold amount of currency, referred to as "covered transactions."

FinCEN has interpreted the definition of financial institutions within its regulations to include residential mortgage lenders and residential mortgage loan originators (jointly: RMLO) as a significant subset of the "loan or finance company" category, thereby subjecting these institutions to the BSA and its regulations. A residential mortgage lender is a person to whom the debt arising from a residential mortgage loan is initially payable or the obligation is initially assigned at or immediately after the settlement of the loan. A residential mortgage loan originator is a person whom accepts a residential mortgage loan application or offers or negotiates terms of a residential mortgage loan for compensation or gain. Mortgage brokers are included within this definition.

2 General Requirements for Compliance

The foregoing BSA/AML policy serves a dual purpose. First, the policy establishes guidelines for compliance with the Bank Secrecy Act. Second, the policy establishes steps for fraud mitigation. The controls and processes put into place by this policy seeks to identify and mitigate activities that constitute fraud, or serve to conceal fraud. Activities that serve to conceal fraud must be escalated and investigated as suspicious activities.

The BSA does not require the institution to take action, other than reporting a transaction reported as a suspicious activity. It is the sole discretion of the institution to alter or terminate its relationship with entities who have been identified as engaging in suspicious activities. Senior management reserves the authority to make those business decisions. The institution shall implement its BSA/AML policy in order to detect and report covered transactions in consideration of the institution's unique risks arising from its products and services offered. Other considerations include the business size, geographic markets served, and service delivery channels.

The compliance program must be approved by the company's executives, board of directors, fiduciary advisors, and provide for the following minimum requirements:

- Development of internal policies, procedures, and controls to identify suspicious transactions and report them accordingly.
- Designation of a BSA/AML compliance officer.
- Ongoing employee training.
- Periodic independent testing of the program.
- In addition, a customer identification program must be included as part of the BSA/AML compliance program.

3 Money Laundering

Financial institutions and RMLOs are in a position where they may likely be exposed to all three stages of money laundering simultaneously in a home purchase, refinance transaction, or progressively through ongoing mortgage payments. For purposes of the institution's compliance efforts, money laundering shall be defined as conducting a financial transaction with the proceeds of an illegal activity to:

- Promote an illegal activity.
- Evade federal income taxes.
- Conceal or disguise the nature, location, source, ownership or control of the illegal proceeds, or
- Avoid a transaction reporting requirement under state or federal law.

There are three essential steps in an attempt to launder money, these steps may occur independently or simultaneously:

- Placement: the physical placing of cash, illegal proceeds, into a legitimate commerce, such as a home purchase or mortgage payment.
- Layering: the separating of the source of cash from its criminal origins by passing it through several financial transactions.
- Integration: the aggregating of funds or cash with legitimately obtained funds and providing a legitimate explanation for its ownership.

4 BSA/AML Violations

Repeated, regular, usual, or institutionalized practices will typically constitute a pattern or practice. The totality of the circumstances will be considered when assessing whether a pattern or practice exists. Types of systemic or recurring violations may include, but are not limited to:

1. Failure to establish a due diligence program that includes a risk-based approach, and when necessary, enhanced policies, procedures, and controls concerning foreign correspondent accounts.

2. Failure to maintain a reasonably designed due diligence program for private banking accounts for non-U.S. persons (as defined in 31 CFR § 103.175).

3. Frequent, consistent, or recurring late Currency Transaction Report (CTR) or SAR filings.

4. A significant number of CTRs or SARs with errors or omissions of data elements.

5. Consistently failing to obtain or verify required customer identification information at account opening.

6. Consistently failing to complete searches on 314(a) information requests.

7. Failure to consistently maintain or retain records required by the BSA.

Isolated or technical violations are limited instances of noncompliance with the BSA that occur within an otherwise adequate system of policies, procedures, and processes. These violations generally do not prompt serious regulatory concern or reflect negatively on management's supervision or commitment to BSA compliance, unless the isolated violation represents a significant or egregious situation or is accompanied by evidence of bad faith.

5 Management Responsibilities

The institution's Board of Directors, stakeholders and senior management are responsible for the company's overall compliance with the BSA and its regulations, particularly the establishment of a BSA/AML Compliance Program and the appointment of a qualified BSA/AML Compliance Officer to oversee the program. The Board of Directors and management should create a culture of compliance to ensure staff adherence to the institution's BSA/AML policies, procedures, and processes.

Senior management shall take any action it deems necessary to protect the interests of the institution as a result of a suspicious activity being reported. Such action may include termination or suspension of the institution's relationship with the reported individual or entity. Additionally, the Board of Directors and senior management must ensure that the BSA/AML Compliance Officer is supported with adequate resources to carry out the program in an effective and meaningful manner. Any updates and changes to the program shall be first approved by senior management.

The institution shall appoint a specific individual to serve as the company's BSA /AML Compliance Officer that, as such, is responsible for the effective implementation and ongoing oversight of the BSA/AML Compliance Program.

The Board of Directors is responsible for ensuring that the BSA compliance officer has sufficient authority and resources (monetary, physical, and personnel) to administer an effective BSA/AML compliance program based on the institution's risk profile. The BSA/AML Compliance Officer shall:

- Oversee and facilitate any necessary investigations related to fraud and other suspicious activities

- Periodically report to senior management regarding any submissions to Fincen and any updates to the program

- Serve as the point of contact between the regulatory and enforcement agencies as it relates to any BSA submissions and examinations of the compliance program

- Subsequent to the required risk assessment, the compliance officer shall review the program and suggest enhancements and other required maintenance of the program to senior management

The BSA/AML Compliance Officer is responsible for ensuring that appropriate employees undergo training on their obligations under the BSA and the institution's BSA/AML Compliance program. The BSA/AML Compliance Officer shall receive periodic training appropriate to the institution's risk profile, products and services offered, and changes to regulatory requirements.

6 Internal Controls and Risk Assessment

The institution's policies, procedures and processes are designed to limit risks and to achieve compliance with the BSA. Internal controls should:

1. Identify vulnerable banking operations (ie, products, services, customers, entities, and geographic locations); provide for periodic updates to the institution's risk profile; and provide for a BSA/AML compliance program tailored to manage risks.

2. Inform the Board of Directors and senior management of compliance initiatives, identified compliance deficiencies, and corrective action taken; and notify directors and senior management of SARs filed.

3. Identify a person or persons responsible for BSA/AML compliance.

4. Provide for program continuity despite changes in management or employee composition or structure.

5. Meet all regulatory recordkeeping and reporting requirements, meet recommendations for BSA/AML compliance, and provide for timely updates in response to changes in regulations.

6. Implement risk-based Customer Due Diligence policies, procedures, and processes.

7. Identify reportable transactions and accurately file all required reports including SARs, CTRs, and CTR exemptions.

8. Provide for dual controls and the segregation of duties to the extent possible.

9. Provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity.

10. Provide for adequate supervision of employees engaged in any activity covered by the BSA and its implementing regulations.

11. Incorporate BSA compliance into the job descriptions and performance evaluations, as appropriate.

12. Train employees to be aware of their responsibilities under the BSA regulations and internal policy guidelines.

The institution's risk assessment should list and identify characteristics for:

- Loans originated by the company and/or agents.
- Loans purchased from other companies.
- Loans serviced, not owned by the company.

The institution shall conduct a risk assessment of the company's exposure to suspicious or criminal activity, fraud, and large value currency transactions related to the products and services offered. The assessment should be conducted at least as often as the independent testing of the BSA/AML Compliance Program. the institution's assessment shall at least consider the following factors:

- New products or services offered.
- Existing products and services offered.
- Number of loans offered since previous assessment.
- The markets served.
- Geographic locations of properties involved in transactions.

- Geographic locations of clients involved in transactions.
- Turnover of key personnel.
- Reliance on third party vendors.
- Regulatory changes.
- Instances of mortgage fraud, or attempted mortgage fraud.
- Any other risks posed to the company identified by senior management or the BSA/AML Compliance Officer.

The results of the risk assessment will be presented to the Board of Directors and senior management. This presentation allows for input by management concerning potential changes to the BSA/AML Compliance Program. As needed, the institution will enhance its procedures at the department or process level to ensure risks identified in the risk assessment are adequately addressed and mitigated. Such enhancements should be done in coordination with the BSA/AML Compliance Officer and communicated to senior management.

7 Customer Identification Program

The institution must have a written Customer Identification Program (CIP). The CIP rule implements section 326 of the USA Patriot Act and requires each institution to implement a written CIP that is appropriate for its size and type of business and that includes certain minimum requirements. The CIP must be incorporated into the BSA/AML compliance program, which is subject to approval by the Board of Directors.

The CIP is intended to enable the institution to form a reasonable belief that it knows the true identity of each customer. The CIP must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer. the institution should conduct a risk assessment of their customer base and product offerings, and in determining the risks; consider:

- The types of accounts offered by the institution.
- the institution's methods of opening accounts.
- The types of identifying information available.
- the institution's size, location, and customer base, including types of products and services used by customers in different locations.

At a minimum, the institution must obtain the following identifying information from each customer before opening the account:

- Name.
- Date of birth for individuals.
- Address.
- Identification number.

The CIP must contain risk-based procedures for verifying the identity of the customer within a reasonable period of time after the account is opened. An institution using documentary methods to verify a customer's identity must have procedures that set forth the minimum acceptable documentation. The rule reflects the federal banking agencies' expectations that institutions will review an unexpired government-issued form of identification from most customers.

The institution shall require that personnel review more than a single document to ensure a reasonable belief that it knows the customer's true identity. The institution is not required to use non-documentary methods to verify a customer's identity. However, an institution using non-documentary methods to verify a customer's identity must have procedures that set forth the methods to be used. The institution's non-documentary procedures must also address the following situations:

1. An individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard.
2. The institution is not familiar with the documents presented.
3. The account is opened without obtaining documents.
4. The customer opens the account without appearing in person.
5. the institution is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents.

The CIP must also have procedures for circumstances in which the institution cannot form a reasonable belief that it knows the true identity of the customer. These procedures should describe:

1. Circumstances in which the institution should not open an account.

2. The terms under which a customer may use an account while the institution attempts to verify the customer's identity.

3. When the institution should close an account, after attempts to verify a customer's identity have failed.

4. When the institution should file a SAR in accordance with applicable law and regulation.

8 Customer Due Diligence

The institution must implement customer due diligence (CCD) procedures. The objective of CDD should be to enable the institution to predict with relative certainty the types of transactions in which a customer is likely to engage. These processes assist the institution in determining when transactions are potentially suspicious. The concept of CDD begins with verifying the customer's identity and assessing the risks associated with that customer. Processes should also include enhanced CDD for higher-risk customers and ongoing due diligence of the customer base. BSA/AML policies, procedures, and processes should include CDD guidelines that:

1. Are commensurate with the institution's BSA/AML risk profile, paying particular attention to higher-risk customers.

2. Contain a clear statement of management's overall expectations and establish specific staff responsibilities.

3. Ensure that the institution possesses sufficient customer information to implement an effective suspicious activity monitoring system.

4. Provide guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.

5. Ensure the institution maintains current customer information.

9 Employee Training

At least annually, appropriate personnel shall receive periodic and ongoing training regarding their responsibilities under the BSA and the BSA/AML Compliance Program. Training may be provided by the BSA/AML Compliance Officer or external training services, at the discretion of the BSA/AML Compliance Officer. The BSA/AML Compliance Officer is responsible for ensuring that new employees are aware of the institution's BSA/AML Compliance Program and their corresponding responsibilities.

Training should focus on the employees' responsibilities to identify covered transactions, any changes to procedures that involve covered transactions, the process of reporting to the FinCEN and IRS, the obligation to maintain confidentiality of a report, and provide examples of potential transactions subject to reporting for the employees involved in training.

Training should include regulatory requirements and the internal BSA/AML policies, procedures, and processes of the institution. At a minimum, the institution's training program must provide training for all personnel whose duties require knowledge of the BSA. Training for employees shall culminate with a test of the BSA/AML Compliance Program.

The Board of Directors and senior management shall be kept up to date on regulatory requirements of the BSA, ramifications for violations or noncompliance with the BSA, results of the risk assessment, and any changes to the BSA/AML Compliance Program. This may be done via official training sessions or through the BSA/AML Compliance Officer's periodic reporting. If the training is done via the periodic reporting, then a copy of the report and presentation should be documented with the training materials.

In addition, an overview of the BSA/AML requirements typically should be given to new staff during employee orientation. Training should encompass information related to applicable business lines. While the Board of Directors may not require the same degree of training as banking operations personnel, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed to the institution. The training program should reinforce the importance that the board and senior management place on compliance with the BSA and ensure that all employees understand their role in maintaining an effective BSA/AML compliance program. The following must be addressed in the training program and materials:

1. The importance the Board of Directors and senior management place on ongoing education, training, and compliance.

2. Employee accountability for ensuring BSA compliance.

3. Comprehensiveness of training, considering specific risks of individual business lines.

4. Training of personnel from all applicable areas.

5. Frequency of training.

6. Documentation of attendance records and training materials.

7. Coverage of institutional policies, procedures, processes, and new rules and regulations.

8. Coverage of different forms of money laundering and terrorist financing as it relates to identification and examples of suspicious activity.

9. Penalties for noncompliance with internal policies and regulatory requirements.

The BSA/AML Compliance Officer shall track and document employee training. The tracking and documenting shall include records of employees who received training, training materials presented, and test results; such records shall be retained for at least five (5) years.

10 Independent Testing

The institution's BSA/AML Compliance Program must be independently tested external auditors, consultants, or other qualified independent parties every twelve (12) to eighteen (18) months. The independence of the tester shall be acceptable so long as the individual is not the BSA/AML Compliance Officer or does not report to the BSA/AML Compliance Officer. The independent testing shall, at a minimum, include:

1. A risk-based evaluation of the effectiveness of the institution's BSA/AML compliance program.

2. A review of the institution's risk assessment based on its risk profile.

3. A review of the institution's adherence to BSA/AML reporting requirements via transaction testing.

4. A review of staff training.

5. An evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations.

6. A review of any other matters considered significant or requiring attention.

7. An assessment of the overall process for identifying and reporting suspicious activity, including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness, and effectiveness of the institution's policy.

8. An assessment of the integrity and accuracy of MIS used in the BSA/AML compliance program. MIS includes reports used to identify large currency transactions, aggregate daily currency transactions, funds transfer transactions, monetary instrument sales transactions, and analytical and trend reports.

11 BSA Reporting Requirements

The institution is not obligated by the BSA to resolve the suspicious activity; rather, the institution need only reasonably attempt to identify the parties involved and detail why the transaction was suspicious. Institutions are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing, and certain other crimes above prescribed dollar thresholds. However, institutions are not obligated to investigate or confirm the underlying crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, and various types of fraud).

Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity. the institution should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities, taking into account the institution's overall risk profile and the volume of transactions.

FinCEN's final rule provides guidance that RMLOs will most often file SARs regarding fraudulent attempts to obtain a mortgage or launder money by use of the proceeds of other crimes to purchase residential real estate.

Banks, institutional holding companies, and their subsidiaries are required by federal regulations to file a SAR with respect to:

1. Criminal violations involving insider abuse in any amount.

2. Criminal violations aggregating $5,000 or more when a suspect can be identified.

3. Criminal violations aggregating $25,000 or more regardless of a potential suspect.

4. Transactions conducted or attempted by, at, or through the institution (or an affiliate) and aggregating $5,000 or more, if the institution or affiliate knows, suspects, or has reason to suspect that the transaction:

    a) May involve potential money laundering or other illegal activity (e.g., terrorism financing).

    b) Is designed to evade the BSA or its implementing regulations.

    c) Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Policies, procedures, and processes should describe the steps the institution takes to address each component and indicate the person(s) or department(s) responsible for identifying or producing an alert of unusual activity, managing the alert, deciding whether to file, and SAR completion and filing. Employees acquiring information for a potential SAR should keep questioning in line with the usual verification procedures used in the transaction.

In order to effectively complete a SAR, the employee encountering a suspicious transaction should obtain the following information:

1. The parties involved in the suspicious activity.
2. The nature of the transaction.
3. The suspicious activity.
4. When and where the suspicious activity occurred.
5. When the transaction originated.
6. Why the activity was suspicious.
7. How the suspicious activity was uncovered; and
8. The institution's response.

Additionally, the institution may elect to file a SAR regarding any transaction it believes is relevant to the possible violation of any law or regulation, but who's reporting is not required by the BSA.

12 SAR Completion and Filing

The institution should implement appropriate training, policies, and procedures to ensure that personnel adhere to the internal processes for identification and referral of potentially suspicious activity. At no point in time should any employee convey to a third party that the information is being gathered to complete a SAR.

An employee who encounters a potentially suspicious transaction should inform the BSA/AML Compliance Officer as soon as possible. The BSA/AML Compliance Officer, in consultation with senior management and other appropriate internal parties, shall determine whether the transaction requires a SAR once all of the information required for a report is obtained or, should all of the necessary information not be available after reasonable investigation, prior to the 30 day deadline to file.

If no suspect can be identified on the date of initial detection, then the institution must complete the SAR to the best of its ability and submit the report within 60 days of the initial detection. If a situation occurs that requires immediate attention, i.e. terrorist financing or ongoing money laundering schemes, then the institution should report the instance immediately to law enforcement authorities as well as appropriately file the SAR.

The time period for filing a SAR starts when the organization, during its review or because of other factors, knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity.

It is important to document the responses and resolutions of the institution as it relates to transactions that are reported as SARs and those transactions that are eventually determined to be not suspicious, for instance those transactions that, after reasonable investigation by employees, are determined not suspicious. the institution are required to file SAR forms that are complete, thorough, and timely. Because the SAR narrative section is the only area summarizing suspicious activity, the section, as stated on the SAR form, is "critical." Thus, a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

SARs are required to be submitted electronically. The BSA/AML Compliance Officer shall register for the BSA E-filing tool in order to submit the documents appropriately. At least one member of senior management, other than the BSA/AML Compliance Officer, shall register as an e-filer in order to avoid any conflicts should the BSA/AML Compliance Officer be the employee who identified the suspicious transaction or the suspect of a SAR.

13 Supervisory Examination Procedures

As part of its recurring compliance examination, the institution is subject to a review of its BSA/AML program. Examination Procedures are intended to assess the overall effectiveness of a RMLO's BSA/AML Program and compliance with BSA, OFAC, CIP, and Identify Theft Prevention regulatory requirements. State compliance examiners will request and review the items outlined below, which aligns with the information request of the Multistate Mortgage Committee Examination Procedures, implemented by the Conference of State Bank Supervisors.

14 BSA/AML Examination Checklist

1	Documentation of Board or senior management approval of the BSA/AML Program and Compliance Officer.
2	Copy of the most recent written BSA/AML Program approved by the Board or senior management, including CIP, with date of approval noted in any meeting minutes.
3	How often are BSA/AML reports presented to the Board?
4	Copies of the last two BSA/AML Program risk assessments.
5	Associated policies, procedures, and controls applicable to BSA/AML, CIP, OFAC, and Identity Theft Prevention.
6	Copies of all policies and procedures relating to reporting and recordkeeping requirements, including suspicious activity reporting.
7	Name, title, resume and qualifications of the designated BSA compliance officer and any other staff responsible for monitoring BSA/AML compliance. *(Resume should include start date as BSA Compliance Officer and list BSA/AML specific training completed during the exam period.)*
8	Name, title, resume and qualifications of the designated OFAC compliance officer and any other staff responsible for monitoring OFAC compliance. (if different from #5)
9	Copies of the last two BSA/AML Program independent tests/audits, including the scope of the testing and the qualifications of the auditors (external or internal) who performed the independent test/audit.
10	Management response to the last two independent tests/audits, including any document tracking, assigned personnel, required actions, recommendations, corrective actions, due dates, and status tracking.
11	BSA/AML training documentation, including training materials, schedule, attendees, and topics covered.
12	An excel spreadsheet of all employees (including senior management and the board) that includes: 1) Name, 2) Title, 3) Hire Date, 4) Dates of previous two BSA/AML trainings.
13	Report/Log of Suspicious Activity Reports (SAR) filed during the examination period. (*can be provided on-site*).
14	Report/log of unusual activity that was reviewed but deemed not suspicious (*can be provided on-site*).

15	Selection of SARs filed with FinCEN, including any supporting documentation and copies of any filed SARs that were related to section 314(a) requests for information or to section 314(b) information sharing requests (*can be provided on-site*).
16	Any analyses or documentation of activity for which a SAR was considered but not filed, or for which the RMLO is actively considering filing a SAR (can be provided on-site).
17	Any information sharing correspondence between the RMLO and state or federal agencies or other financial institutions (if applicable).
18	Does the RMLO uses a manual or automated suspicious activity monitoring system, or a combination of the two?
19	If an automated system is used, indicate whether the system is proprietary, or vendor supplied and whether the system is incorporated within the Loan Origination System (LOS) and whether the LOS is proprietary, or vendor supplied.
20	If the system is vendor supplied, provide the name of the vendor and system, and installation/plug-in dates
21	Has the RMLO filed any Report of Foreign Bank and Financial Accounts (FBAR)?
22	Has the RMLO filed any Form 8300s?
23	Does the RMLO have a list of blocked or rejected transactions with individuals or entities on the OFAC list and reported to OFAC? *(If maintained, make available logs or other documentation related to reviewing potential OFAC matches, including the method for reviewing and clearing those determined not to be matches.*