MMC MORTGAGE EXAMINATION MANUAL
BSA/AML PROGRAM EXAMINATION PROCEDURES

Bank Secrecy Act/Anti-Money Laundering (BSA/AML)

Office of Foreign Assets Control (OFAC)

Customer Identification Program (CIP)

Identity Theft Prevention

MULTISTATE MORTGAGE COMMITTEE
1129 20th Street, NW, Ninth Floor
Washington, D.C. 20036
(202) 728-5756
www.csbs.org

Acronyms

AML	Anti-Money Laundering
BSA	Bank Secrecy Act
CIP	Customer Identification Program
EFE	Elder Financial Exploitation
EIC	Examiner-In-Charge
FBAR	Foreign Bank and Financial Accounts Report
FBI	Federal Bureau of Investigation
FCRA	Fair Credit Reporting Act
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network
FTC	Federal Trade Commission
GSE	Government-Sponsored Enterprise
HIDTA	High Intensity Drug Trafficking Area
HIFCA	High Intensity Financial Crime Area
LOS	Loan Origination System
IRS	Internal Revenue Service
OFAC	Office of Foreign Assets Control
ROE	Report of Examination
RMLO	Residential Mortgage Lenders and Originators
SAR	Suspicious Activity Report
Secretary	Secretary of the Treasury

Revisions

This MMC Mortgage Examination Manual – BSA/AML Program Examination Procedures is subject to revision as needed. All revisions are announced and made available to each regulatory jurisdiction. Any suggested revisions to these Examination Procedures can be submitted via email for MMC consideration at MMCSupport@csbs.org.

Version 2 Updates – Fall 2019
Added sections specific to OFAC, CIP and Identify Theft Prevention;
Updated regulatory references and resources;
Added key risk factors descriptions for BSA/AML Programs;
Added suspicious activity examples for RMLOs;
Enhanced SAR narrative specific to RMLOs;
Added Scope and Planning section;
Updated BSA/AML Examination Procedures and added examination procedures specific to OFAC, CIP and Identify Theft Prevention;
Removed separate definitions section.

Table of Contents

For the purposes of these Examination Procedures, the review of a RMLO's BSA/AML Program also includes a review of OFAC, CIP, and Identity Theft Prevention associated policies, procedures and processes.

Prior to completing the BSA/AML Program Examination Procedures, state agencies that regulate and examine RMLOs should review their specific state financial codes for applicable authority to examine for the following:

Name	Regulation	Additional Links
Bank Secrecy Act (BSA)	31 CFR Chapter X	FinCEN Mandate
FCRA Identity Theft Rules	16 CFR Part 681	FTC Red Flags Rule
Office of Foreign Assets Control (OFAC)	NA	Treasury OFAC
USA PATRIOT Act	Public Law 107-56	FinCEN USA PATRIOT Act

Bank Secrecy Act / Anti-Money Laundering (BSA/AML)

Introduction

Residential mortgage lenders and originators (RMLOs) are in a unique position to assess and identify money laundering risks, fraud, and other forms of potential suspicious activity. As a first line of defense, RMLOs can readily identify suspicious transactions and activities since they work closely with consumers when originating, underwriting, and approving or denying mortgage loans. The Financial Crimes Enforcement Network (FinCEN) expanded the applicability of the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) regulations to include nonbank RMLOs in 2012[1].

The expansion imposed specific BSA and AML protocols on any RMLO who makes or acquires loans secured by deeds of trust or mortgages on residential properties. Specifically, FinCEN requires each RMLO to create and implement a risk-based BSA/AML compliance program (BSA/AML Program), train their employees on money-laundering and fraud, and file Suspicious Activity Reports (SARs).

RMLOs are defined in the Bank Secrecy Act[2] as follows:

- **Residential mortgage lender.** The person to whom the debt arising from a residential mortgage loan is initially payable on the face of the evidence of indebtedness or, if there is no such evidence of indebtedness, by agreement, or to whom the obligation is initially assigned at or immediately after settlement. The term "residential mortgage lender" shall not include an individual who finances the sale of the individual's own dwelling or real property.

[1] FinCEN is responsible for the management of RMLO BSA/AML programs and has delegated the responsibility of examining RMLOs to the IRS. FinCEN, 31 CFR Parts 1010 and 1029*: Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Residential Mortgage Lenders and Originators*

[2] See 31 CFR §1010.100(lll)(1)

- **Residential mortgage originator.** A person who accepts a residential mortgage loan application or offers or negotiates terms of a residential mortgage loan.
- **Residential mortgage loan.** A loan that is secured by a mortgage, deed of trust, or other equivalent consensual security interest on:
    - A residential structure that contains one to four units, including, if used as a residence, an individual condominium unit, cooperative unit, mobile home or trailer; or
    - Residential real estate upon which such a structure is constructed or intended to be constructed

BSA/AML Program Requirements

31 CFR §1029.210 requires RMLOs to develop and implement a written BSA/AML Program to include policies, procedures, and controls that are designed to prevent, detect, and deter money laundering and terrorist financing. The Program must be approved by senior management or the Board of Directors, depending on the corporate structure of the RMLO.

At a minimum, the BSA/AML Program should include the following four "pillars":

1) Policies, procedures, and internal controls based on an assessment of risks associated with products, services, customer types and geographic locations;
2) Designation of a qualified compliance officer responsible for ensuring day-to-day compliance:
3) On-going training of appropriate persons concerning their responsibilities under the Program; and
4) Independent testing and audit functionality to monitor and maintain an adequate Program.

BSA/AML Programs must be *risk-based* and developed proportionate to the size, and complexity of each RMLO. Thus, each BSA/AML Program will vary due to different products and services, geographic locations, customer types, and other risks.

A *risk-based* approach requires RMLOs to identify inherent risks associated with its day-to-day operations and to have systems and controls that are commensurate with the specific risks they face. Assessing this risk is therefore one of the most important steps in creating an effective and compliant BSA/AML Program.

The Financial Action Task Force (FATF) urges *risk-based* controls because they are more *flexible*, *effective* and *proportionate*[3]. The theory is that no financial institution can reasonably be expected to detect all wrongdoing by customers, but if a financial institution develops systems and procedures to detect, monitor and report the riskier customers and

[3] See *FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing* (issued 6/07)

transactions, it will increase its chances of effectively identifying and reporting suspicious activity and decrease its chances of facing scrutiny or penalties.

As risks are identified, the BSA/AML Program needs to be reviewed and enhanced to incorporate stronger controls as necessary. RMLOs must conduct an effective risk assessment to appropriately identify high-risk operations unique to its business. Although risk can originate from many different sources, the core primary risk factors to assess include an RMLO's products and services, customer types, and geographic locations.

Depending on the size of the RMLO, the BSA/AML Program may be managed by an individual employee (i.e. the designated compliance officer), a stand-alone department, or integrated into another department such as compliance or risk. Regardless of size, the BSA/AML Program should have a corporate-wide view of its BSA/AML efforts.

Internal Policies, Procedures and Controls

Internal policies should be established and approved by the board of directors or senior management and should set the tone for the organization (see **Culture of Compliance**).

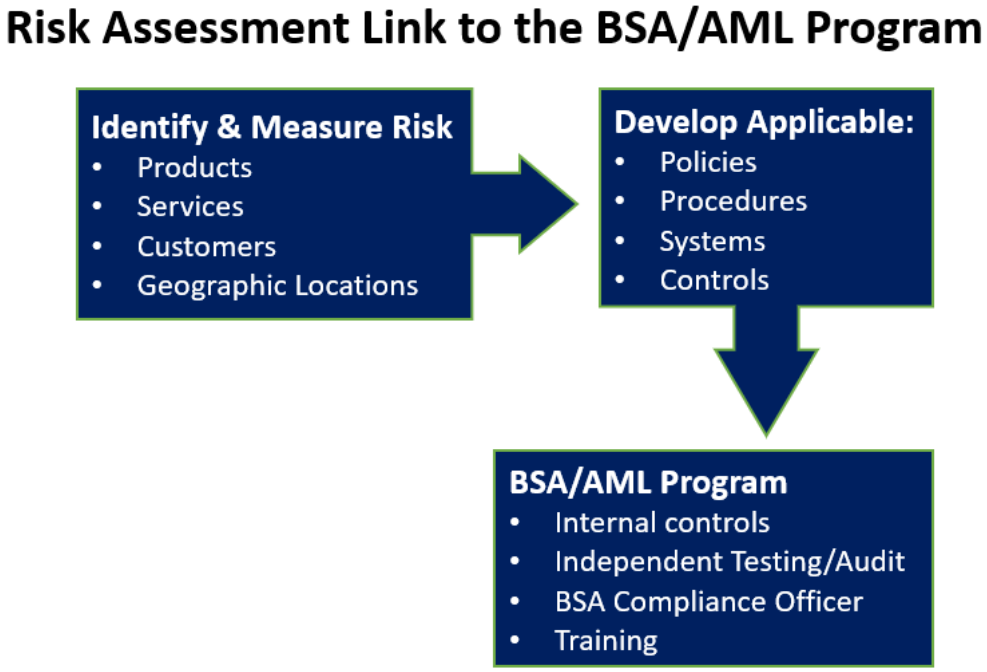
The internal policies serve as the basis for procedures and controls and provide details as to how the RMLO will comply with and all applicable laws and regulations, as well as its BSA/AML Program. While policies and procedures provide important guidance, the BSA/AML Program also relies on internal controls, including management reports and other safeguards.

The internal policies, procedures, and controls should be commensurate with the size and complexity of the company and be based upon the risks associated with its products and services, customer types, geographic locations, and any other identified risk factors. The internal policies, procedures, and controls developed and implemented must consider the RMLO's agents and brokers and include requirements for obtaining all relevant customer-related information necessary for an effective BSA/AML Program, as required by 31 CFR 1029.210.

As a best practice RMLO's should conduct risk assessments prior to developing a BSA/AML Program. The risk assessment should be reviewed on a regular basis in order to maintain updated and accurate information, or as specific circumstances warrant, such as the addition of new products and/or services. The risk assessment should identify the RMLO's risk categories and provide a detailed analysis to assess the level of risk within each category.

As a result of conducting risk assessments, a RMLO can effectively incorporate the complete risk profile of its business operation into the BSA/AML Program. Risk assessments also provide the RMLO an invaluable tool to test the effectiveness of its internal policies, procedures and controls, and to make any necessary changes.

The graphic below from the FFIEC BSA/AML Examination Manual[4] highlights how the risk assessment influences the internal controls needed for a comprehensive risk based BSA/AML Program.



Different business activities will pose a greater BSA/AML risk than others. For example, any activities that are customer-facing (i.e. originating and processing), will be more likely to come across BSA/AML risk such as mortgage fraud and other suspicious activity than administrative functions. RMLOs can develop corporate-wide policies, procedures, and controls as part of its overall BSA/AML Program, but each business channel should have its own set of BSA/AML procedures and controls specific to the activities it performs.

The establishment and continual development of policies, procedures, and controls are foundational to a successful BSA/AML Program. At a minimum, the BSA/AML Program should include the following:

- Identification of high-risk operations (products, services, channels, customers, and geographic locations)
- Procedures and controls tailored to manage the operational risks;
- Clear accountability lines and responsibilities to ensure that there is appropriate and effective oversight of staff who engage in activities which pose a greater BSA/AML risk;
- Training requirements and standards in order to ensure that personnel are made aware of and have a working understanding of the procedures to be followed and their relevance to mitigating BSA/AML risks in their specific business channels (department) or areas of responsibilities;

[4] FFIEC BSA/AML Examination Manual: Appendix I (accessed 9/19/19)

- Procedures for reporting suspicious activity, including describing how to appropriately escalate and report the suspicious the activity internally; and
- Job descriptions and performance review processes that incorporate the requirement to comply at all times with BSA/AML policies and procedures and repercussions for non-compliance.

Designation of a BSA Compliance Officer

The board of directors or senior management is responsible for appointing a qualified individual to serve as the BSA/AML compliance officer and ensuring that this individual has sufficient authority and resources (monetary, physical, and personnel) to administer an effective BSA/AML Program based on the company's risk profile.

This individual is responsible for managing all aspects of the BSA/AML Program, which includes implementing the Program, making necessary changes and updates, disseminating information, ensuring appropriate personnel receive training, and managing the company's adherence to applicable laws and regulations (BSA, CIP, OFAC, ID Theft Prevention Rules).

The ability of the compliance officer to communicate effectively, both in writing (needed to develop effective SAR narratives) and verbally, is vital to the success of an effective BSA/AML Program. The compliance officer must also have the means to communicate at all levels of the organization as it is critical for this individual to be able to escalate urgent matters of importance to senior management and the board so that management can make informed decisions about overall BSA/AML compliance.

The BSA Compliance Officer can delegate BSA/AML duties to other personnel, but the compliance officer is ultimately responsible for the BSA/AML Program and applicable laws and regulations. It is critical for the compliance officer to be fully knowledgeable of all BSA/AML regulations and understand how the RMLO's products, services, customers, geographic locations and other activities may affect money laundering, terrorist financing, mortgage fraud, and other illegal activity risk.

Additionally, the compliance officer should receive timely training relevant to their BSA/AML duties. The designation of a compliance officer is not sufficient to meet the regulatory requirement if that person does not have the expertise, authority, or time to satisfactorily complete the job.

Training

The RMLO must ensure that appropriate personnel are trained on the BSA/AML Program for their respective roles. Training should include all applicable regulatory requirements and the company's BSA/AML Program policies, procedures, and controls. At a minimum, the RMLO's training program must provide training for all personnel whose duties require knowledge of the BSA/AML Program. An effective training program should be tailored to the specific responsibilities of personnel.

Below is an example of how a RMLO may conduct company-wide and operational-specific training that incorporates the Three Lines of Defense model used for organizing governance, risk management and internal control roles and responsibilities[5]. According to the model, the first line of defense in risk management consists of controls within the public-facing operations. Risk management and compliance oversight functions operate as the second line of defense. Independent testing and internal audit make up the third line. These three lines play a specific role within a RMLO's risk management program:

- First line primarily owns and manages risk;
- Second line monitors and oversees risk; and
- Third line provides independent assurance of the risk management and risk monitoring provided by the first and second lines of defense.

Training Structure Example:

- **Company-wide:** A general knowledge course that addresses the importance of applicable regulations and how its BSA/AML Program complies with those regulations. This training ensures all RMLO employees are aware of BSA/AML requirements even though they may not be directly involved in the front-line operations. Examples include administrative support and human resources.
- **Customer-facing employees:** This is a RMLO's first line of defense and includes the employees who need the most practical understanding of why BSA/AML efforts are important and what they need to do to be vigilant against mortgage fraud and other suspicious activity. Examples include mortgage loan originators and loan processors.
- **Operations employees:** Non-customer facing personnel that handle loan files and documentation provided by customers and third parties are also included in the first line of defense. Examples include underwriters, pre- and post-closers and servicing staff.
- **BSA/AML and compliance employees:** Although this is considered a second line of defense, these employees are responsible for managing the BSA/AML Program, so more advanced ongoing training to stay abreast of requirements and emerging trends is important.
- **Independent testing employees:** Independent testing employees are the organization's third line of defense. Because this functional area independently assesses the adequacy of the BSA/AML Program, these employees should receive periodic training concerning regulatory requirements and how changes to applicable regulations impact the BSA/AML Program and their organization.
- **Senior management and board of directors:** Management does not need the same degree of training as personnel in the first, second or third lines of defense. Specialized training for leadership should address the importance of BSA/AML regulatory requirements, penalties for noncompliance, personal liability, and the organization's unique risks. Without a general understanding of this information,

[5] Institute of Internal Auditors (IIA) Position Paper: *The Three Lines of Defense in Effective Risk Management and Control* (published 1/13)

senior management and/or the board cannot adequately provide for BSA/AML oversight, approve BSA/AML policies, or provide sufficient resources or support.

BSA/AML training should be ongoing and on a regular schedule. Existing employees should receive training at last annually and new employees should receive appropriate training within a reasonable period after joining the company. The training program should reinforce the importance of the BSA/AML Program and ensure that all employees understand their role in maintaining an effective Program. A RMLO may satisfy this requirement by directly training its employees, agents, and brokers or verifying that such persons have received relevant training by a competent third party.

Situations may arise that may require new or updated training immediately. For example, a training may be necessary right after an examination or audit uncovers serious deficiencies with mortgage fraud controls. Additionally, any changes to policies, procedures, or controls may trigger new or updated training.

The RMLO should document its BSA/AML training. Documentation should include the training materials (i.e. videos, slides, scripts, etc.), testing materials, the dates of training sessions, and attendance. Documentation should be maintained and be available for examiner review.

Independent Testing

The BSA/AML Program must be monitored and evaluated through independent testing. The independent testing can be conducted by internal staff, outside auditors, consultants, or other qualified independent parties. Regardless of who performs the independent testing, it cannot be performed by the designated BSA compliance officer or any staff with BSA/AML duties. Additionally, individuals conducting the audit should report directly to the board of directors or senior management. Those performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable.

Independent testing should:

- Assess the overall integrity and effectiveness of the BSA/AMP Program, with an emphasis on the Program's policies, procedures and controls;
- Assess the adequacy of the BSA/AML risk assessment;
- Examine the adequacy of the BSA/AML Program procedures and controls and whether they comply with all applicable regulatory requirements;
- Determine personnel compliance and commitment to the BSA/AML Program;
- Perform appropriate testing, with particular emphasis on any known high-risk operations (products, services, customers and geographic locations);
- Assess the adequacy of training, including its comprehensiveness, accuracy of materials, training schedule, attendance tracking and escalation procedures for lack of attendance;
- Examine the integrity and accuracy of any internal or external software or systems used in the BSA/AML Program;

- Review all aspects of any BSA/AML functions performed by third parties, including the qualifications of its personnel, the contract, and their performance;
- Review policies, procedures, and controls for suspicious activity monitoring and how suspicious activity is escalated to BSA/AML personnel;
- Assess the adequacy of recordkeeping and record retention processes;
- Review reports provided to the board or senior management and determine if any decisions or changes were made to the BSA/AML Program;
- Consider whether the board or senior management was responsive to earlier audit findings;
- Determine the adequacy of the following, as they relate to training:
    - The importance the board and senior management place on ongoing education, training and compliance;
    - Employee accountability for ensuring BSA/AML compliance;
    - Comprehensiveness of training related to the risk assessment of each individual business line;
    - Frequency of training including the timeliness of training given to new and transferred employees;
    - Coverage of internal policies, procedures, controls and new rules, regulations and regulatory guidance;
    - Coverage of different forms of red flags and schemes as they relate to identifying suspicious activity;
    - Disciplinary actions taken for noncompliance with the BSA/AML Program.

While there is no specific frequency of audit, it is a good practice to conduct an independent test that is commensurate with the BSA/AML risk profile of the company. Risk-based audit programs will vary depending on the company's size, complexity, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology to name a few

All independent testing, audit, and regulatory reports and recommendations for corrective action must be tracked and regular status reports should be provided to the board or senior management. Failure to properly document and address corrective action can lead to regulatory findings by state or federal examiners.

Risk Factors

BSA/AML Programs need to be risk-based and developed proportionate to the size, complexity, and risk appetite of each RMLO. Each BSA/AML Program should be based on the risks associated with its products and services, customer types, and geographic locations. This section provides guidance on these risk factors that examiners may consider when reviewing a RMLO's BSA/AML Program or associated risk assessments.

Products and Services

New and existing loan products and the RMLO's services must be assessed to determine how it may be used to launder money or be susceptible to suspicious activity, including mortgage fraud. Sample factors that may influence risk in this area include:

- How are mortgage applications submitted (i.e. online vs. face-to-face)
- What mortgage loan products are provided?
- What are the features and unique characteristics of each loan product provided?
- Are products or services targeted to a specific customer type?
- Do processing and underwriting activities and processes vary depending on the business channel, loan product, geographic location or customer type?
- Do any services allow customers to engage in transactions with minimal oversight by the RMLO?
- Do mortgage refinances require less documentation than new mortgage loans?
- Does the RMLO require applicants to provide new identification for a refinance?
- Does the RMLO allow payments to third parties?
- Does the RMLO rely on third parties for any services (i.e. processing or underwriting activities)?
- Is the product or service unusually complex?
- Does the RMLO accept traveler's checks or money orders?

Customer Types

Customer types typically include mortgage loan applicants and borrowers. However, third parties and other service providers are also customers of a RMLO and should be included as "Other Types" of customers for the purposes of identifying risk and incorporating all customer types into the overall BSA/AML Program. "Other Types" of customers can include other RMLOs, brokers, third-party processors or underwriters and mortgage servicers, but it includes any party a RMLO conducts business with. Whether the customer is a consumer (i.e. applicant or borrower) or a business, RMLOs must have effective controls to identify and confirm the identity of the individuals. Any individual who applies for a mortgage loan or conducts business with a RMLO can pose BSA/AML risk and conduct suspicious activity.

Sample factors that may influence risk in this area may include:

- States in which the RMLO is licensed and conducts business;
- Number of mortgage loan applications in each state;
- Current and historic HMDA and ECOA information;
- The business activities conducted with customers;
- Target audience(s) for marketing campaigns;
- Occupations of applicants;
- Customer Identification Program (CIP) controls;
- Volume of mortgage loan applications;

- Retention time of customers (i.e. does the RMLO retain the servicing rights of their borrower's mortgage loans or are they sold in the secondary market?)

Geographic Locations

An important factor in determining BSA/AML risk is identifying where a RMLO is based and where it primarily conducts business. While there is no definitive test for assessing the BSA/AML risks of geographic locations, both the Drug Enforcement Administration[6] and FinCEN[7] identify high intensity financial crime areas, detailed below, that can inform the BSA/AML Program and the geographic location risk assessment.

- The ***High Intensity Drug Trafficking Areas (HIDTA) Program*** was created by Congress with the Anti-Drug Abuse Act of 1988 to provide assistance to federal, state, local, and tribal law enforcement agencies operating in areas determined to be critical drug-trafficking regions of the United States. There are currently 28 HIDTAs, which include approximately 18.3 percent of all counties in the U.S. and a little over 65.5 percent of the U.S. population. HIDTA-designated counties are located in 49 states as well as Puerto Rico, the U.S. Virgin Islands, the District of Columbia, and the Warm Springs Indian Reservation in Oregon.
- The ***High Intensity Financial Crime Areas (HIFCA)*** were first announced in the 1999 National Money Laundering Strategy and the program is intended to concentrate law enforcement efforts at the federal, state, and local level to combat money laundering in designated high-intensity money laundering zones.

Examiners should ensure the RMLO is generating and reviewing loan-level reports as part of its BSA/AML Program – and when conducting a risk assessment – to identify mortgage loan applications (both approved and denied) submitted by customers in each state, near physical branch locations, and potential HIDTA and HIFCA areas. If the RMLO considers HIDTA and HIFCA areas and has physical branches locations within a HIDTA or HIFCA, additional scrutiny should be applied when assessing the BSA/AML Program and any applicable risk assessments.

BSA/AML Program Controls to Identify, Research, and Report Suspicious Activity

Suspicious activity monitoring and reporting are critical internal controls. Proper monitoring and reporting processes are essential to ensuring that a RMLO has an adequate and effective BSA/AML Program. In addition to implementing appropriate policies, procedures, and processes to monitor and identify unusual activity, the sophistication of any monitoring systems should be dictated by the RMLO's risk profile. The RMLO should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities. Monitoring systems typically include employee

[6] High Intensity Drug Trafficking Areas (HIDTA)
[7] High Intensity Financial Crime Areas (HIFCA)

identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or any combination of these.

Appendix S to the FFIEC BSA/AML Examination Manual highlights the five key components of an effective suspicious activity monitoring and reporting system. The components, listed below, are interdependent, and an effective suspicious activity monitoring and reporting process should include successful implementation of each component. Breakdowns in any one or more of these components may adversely affect SAR reporting and BSA/AML compliance.

1. Identification or alert of unusual activity (including employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output);
2. Managing alerts;
3. SAR decision making;
4. SAR completion and filing;
5. Monitoring and SAR filing on continuing activity.

While all five components should be present, the structure and formality of the components may vary depending on the size and risk of the RMLO. The BSA/AML Program should describe the steps the RMLO takes to address each component and indicate the person(s) or departments responsible for identifying or producing an alert of unusual activity, managing the alert, deciding whether to file, SAR completion and filing, and monitoring and SAR filing on continuing activity.

Culture of Compliance

Regardless of its size and business model, any RMLO with a poor culture of compliance is likely to have shortcomings in its BSA/AML Program. The board and senior management must set the tone from the top by openly voicing their commitment to compliance, including its BSA/AML Program. This helps everyone else in the organization see the importance of compliance. Adopting a culture of compliance is the most effective way to prevent easily identified issues from becoming systemic problems.

A RMLO can strengthen its BSA/AML compliance culture by ensuring that:

1) Its leadership actively supports and understands compliance efforts;
2) Efforts to manage and mitigate BSA/AML deficiencies and risks are taken seriously and not compromised by revenue interests;
3) Relevant information from the various departments within the organization is shared with designated staff to further BSA/AML efforts;
4) Adequate resources are devoted to its compliance function;
5) The compliance program is effective by, among other things, ensuring that it is tested by an independent and competent party; and
6) Its leadership and staff understand the purpose of its BSA/AML efforts.

FinCEN describes each of these areas in more detail in an advisory promoting a "culture of compliance" at each financial institution. As part of its BSA/AML Program review, examiners should take into account a RMLO's overall Compliance Management System (CMS) and determine whether a culture of compliance is present at the organization.

- FinCEN Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance (issued 8/11/14)

Office of Foreign Assets Control (OFAC)

Introduction

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and to freeze foreign assets under U.S. jurisdiction[8].

All U.S. persons must comply with OFAC regulations, including: all US citizens and permanent resident aliens, regardless of where they are located; all persons and entities within the United States; and all U.S. incorporated entities and their foreign branches. OFAC sanction programs prohibit transactions and require the blocking of assets of persons and organizations that appear on one of a series of sanctions lists administered by OFAC. OFAC has the power to impose significant penalties on those who are found to be in violation of the blocking orders within each of the sanction programs. While OFAC is not a supervisory agency, it works closely with supervisory agencies at both the federal and state levels.

OFAC requirements are separate and distinct from the BSA, but both OFAC and the BSA share a common national security goal. For this reason, many financial institutions view compliance with OFAC sanctions as related to BSA compliance obligations. Therefore, supervisory examination for BSA compliance is logically connected to the examination of a financial institution's compliance with OFAC sanctions[9].

While OFAC regulations are not part of the BSA, examiners should review the RMLO's policies, procedures and processes for compliance with OFAC sanctions. As part of the scoping and planning procedures, examiners should review the RMLO's OFAC risk assessment and independent testing to determine the extent to which a review should be conducted during the examination. Refer to the **Office of Foreign Assets Control (OFAC) Exam Procedures** beginning on page 66 for more information.

[8] See Office of Foreign Assets Control - Sanctions Programs and Information
[9] Taken from the FFIEC BSA/AML Examination Manual: Introduction (accessed 9/10/19)

OFAC Sanctions Lists

OFAC publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country specific. The sanctions lists are available here and detailed below.

During the mortgage loan origination process and as a prerequisite to loan approval, a RMLO should review OFAC requirements and screen its mortgage loan applicants with the OFAC Sanctions Lists of known or suspected terrorists, narcotics traffickers, and other criminal actors for potential matches. RMLOs must be alert to transactions that involve parties identified on any Sanctions List and report positive matches to OFAC within ten days. A RMLO may also be required to file a SAR depending on the circumstances of the transaction.

Many RMLOs depend on third-party systems to automatically screen its mortgage loan applicants against OFAC sanctions lists. However, it is ultimately the responsibility of the RMLO to identify potential matches and report appropriately.

Specially Designated Nationals List

The SDN list contains thousands of names of individuals and businesses from more 150 countries that the U.S. government considers to be terrorists, international narcotics traffickers, or others covered by U.S. foreign policy and trade sanctions. Under sanctions programs administered by OFAC, financial institutions are prohibited from providing property, or an interest in property, to anyone subject to a sanctions program. Depending on the particular program, this might mean blocking (or freezing) the transaction or rejecting (or returning) the transaction.

Consolidated Sanctions List

The Consolidated Sanctions List includes all non-SDN sanctions lists in a consolidated set of data files. While the consolidated sanctions list data files are not part of OFAC's list of SDN List the records in these consolidated files may also appear on the SDN List.

Additional OFAC Sanctions Lists

In addition to the main SDN List that applies to RMLOs, OFAC maintains the following additional sanctions lists:

- Sectoral Sanctions Identifications List
- Foreign Sanctions Evaders List
- Non-SDN Palestinian Legislative Council List
- Non-SDN Iranian Sanctions List
- List of Foreign Financial Institutions Subject to Part 561

- List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions (CAPTA List)

OFAC Compliance Program

OFAC encourages all persons and entities take a risk-based approach to designing and implementing an OFAC Compliance Program. In general, the regulations that OFAC administers require entities to do the following:

- Block accounts and other property of specified countries, entities, and individuals.
- Prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals.

While not required by specific regulation, but as a matter of sound practice and in order to mitigate the risk of noncompliance with OFAC requirements, RMLOs should establish and maintain an effective, written OFAC Compliance Program that is commensurate with their OFAC risk profile (based on products, services, customers, and geographic locations). The program should identify high-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate an experienced employee or employees as responsible for OFAC compliance, and create training programs for appropriate personnel in all relevant areas.

A fundamental element of a sound OFAC Compliance Program is a risk assessment of specific product lines, customer base, and nature of transactions and identification of the higher-risk areas for potential OFAC sanctions risk. As OFAC sanctions can reach into virtually all areas of its operations, RMLOs should consider all types of transactions, products, and services when conducting their risk assessment and establishing appropriate policies, procedures, and processes. An effective risk assessment should be a composite of multiple factors (as described in more detail below), and depending upon the circumstances, certain factors may be weighed more heavily than others. Once the RMLO has identified its areas with higher OFAC risk, it should develop appropriate policies, procedures, and processes to address the associated risks. RMLOs may tailor these policies, procedures, and processes may be tailored to a specific business line or product[10].

Internal Controls

An effective OFAC Compliance Program should include internal controls for identifying suspect accounts and transactions, as well as reporting blocked and rejected transactions to OFAC. Internal controls should include the following elements:

1) **Identifying and reviewing suspect transactions:** The policies, procedures, and processes should address how the RMLO will identify and review transactions and accounts for possible OFAC violations, whether conducted manually, through

[10] See U.S. Department of Treasury's OFAC FAQs for more information.

interdiction software, or a combination of both. For screening purposes, the RMLO should clearly define its criteria for comparing names provided on the OFAC Sanctions List with its mortgage loan applicants. The policies, procedures, and processes should also address how the RMLO will determine whether an initial OFAC hit is a valid match or a false hit.

2) **Reporting:** An OFAC Compliance Program should also include policies, procedures, and processes for handling validly blocked or rejected items under the various sanctions programs. When there is a question about the validity of an interdiction, RMLOs can contact OFAC by phone or e-hot line for guidance. Most other items should be reported through usual channels within ten days of the occurrence. The policies, procedures, and processes should also address the management of blocked accounts.
3) **Independent Testing:** Each RMLO should conduct an independent test of its OFAC Compliance Program that is performed by the internal audit department, outside auditors, consultants, or other qualified independent parties. The frequency and area of the independent test should be based on the OFAC risk profile or on a perceived risk. The person(s) responsible for testing should conduct an objective, comprehensive evaluation of OFAC policies, procedures, and processes. The audit scope should be comprehensive enough to assess OFAC compliance risks and evaluate the adequacy of the OFAC Compliance Program.
4) **Responsible Individual:** Similar to BSA/AML, it is recommended that a qualified individual be designated to be responsible for the day-to-day compliance of the OFAC Compliance Program, including changes or updates to the various sanctions' programs, and the reporting of blocked or rejected transactions to OFAC and FinCEN. This individual should have an appropriate level of knowledge about OFAC regulations commensurate with the RMLO's OFAC risk profile.
5) **Training:** Each RMLO should provide adequate training for all appropriate employees on its OFAC Compliance Program, including applicable procedures and processes. The scope and frequency of the training should be consistent with the OFAC risk profile and appropriate to employee responsibilities.
6) **Recordkeeping Requirements:** OFAC requires a full and accurate record of each such transaction to be available for examination for at least 5 years after the date of such transaction.

For additional information and guidance on OFAC Compliance Programs, examiners are encouraged to review the following resources:

- Department of the Treasury: A Framework for OFAC Compliance Commitments
- FFIEC BSA/AML Examination Manual: Office of Foreign Assets Control Overview

Customer Identification Program (CIP)

Introduction

Section 326 of the USA PATRIOT Act and 31 CFR §1020.220 requires RMLOs to implement a written Customer Identification Program (CIP) appropriate for its size and type of business. The CIP should be part of the RMLO's overall BSA/AML Program and must be approved by senior management or the board of directors, depending on the corporate structure of the RMLO.

Customer Identification Program Requirements

The CIP must include risk-based procedures for verifying the identity of each customer that enable the RMLO to form a reasonable belief that it knows the true identity of each customer. These procedures must be based on the RMLO's assessment of the relevant risks. RMLOs should conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider:

- The types of products and services offered;
- The methods of opening accounts (i.e. applying for a mortgage loan);
- The types of identifying information available;
- The size, locations, and customer base, including types of products and services used by customers in different geographic locations.

The CIP must contain procedures for opening an account that specify the identifying information that will be obtained from each customer. At a minimum, the following four pieces of information is required from the customer prior to opening an account:

1) Name;
2) Date of birth;
3) Address; and
4) Taxpayer identification number.

Based on its risk assessment, a RMLO may require additional identifying information for certain customers or product lines.

Verification Through Documents

For a RMLO relying on documents, the CIP must contain procedures that set forth the documents that will be used to identify the customer. These documents may include unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport. Given the availability of counterfeit and fraudulently obtained documents, RMLOs are encouraged to review more than a single document to ensure that it has a reasonable belief that it knows the customer's true identity.

Verification Through Nondocumentary Methods

For a RMLO relying on nondocumentary methods, the CIP must contain procedures that describe the non-documentary methods that will be used to identify the customer. These methods may include 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, or other source; checking references with other financial institutions; and obtaining a financial statement.

The nondocumentary procedures must address situations where an individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard; the RMLO is not familiar with the documents presented; the account is opened without obtaining documents; the customer opens the account without appearing in person; and where the RMLO is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents.

Lack of Verification

The CIP must include procedures for responding to circumstances in which the RMLO cannot form a reasonable belief that it knows the true identity of a customer. These procedures should describe:

1) When the RMLO should not proceed with the mortgage loan application;
2) The terms under which a customer may proceed with the loan application while the RMLO attempts to verify the customer's identity;
3) The steps to deny a loan application after attempts to verify a customer's identity have failed; and
4) When the RMLO should file a SAR in accordance with applicable law and regulation.

Customer Notice

The CIP must include procedures for providing customers with adequate notice that the RMLO is requesting information to verify their identities. The notice is adequate if the RMLO provides the notice in a manner reasonably designed to ensure that a customer is able to view the notice, or is otherwise given notice, before opening an account.

Many RMLOs include the notice on their websites, display the notice at their office locations, or include the notice in their initial disclosure packages provided to applicants within 3 business days of receiving a mortgage loan application.

Sample USA PATRIOT Act Notice

Important Information About Procedures for Opening a New Account

To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

Comparison with Government Lists

The CIP must include procedures for determining whether the customer appears on any federal government list of known or suspected terrorists or terrorist organizations. RMLOs comply with this portion of the CIP requirements as part of its OFAC Compliance Program. Refer to **Office of Foreign Assets Control (OFAC) Program** beginning on page 16 for more information.

Recordkeeping and Retention Requirements

The CIP must include procedures for retaining the identifying information obtained (name, address, date of birth, TIN, and any other information required by the CIP) for five years after the date the account is closed (i.e. loan consummation). At a minimum, the record must also include the following:

- A description of any document that was relied on to verify identity, noting the type of document, the identification number, the place of issuance, and, if any, the date of issuance and expiration date;
- A description of the methods and the results of any measures undertaken to verify the identity of the customer; and
- A description of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained.

Reliance on Another Financial Institution

A RMLO is permitted to rely on another financial institution (including an affiliate) to perform some or all of the elements of the CIP provided that:

- The relied-upon financial institution is subject to a rule implementing the AML program requirements of 31 USC 5318(h) and is regulated by a federal functional regulator.
- The customer has an account or is opening an account at the RMLO and at the other functionally regulated institution.
- Reliance is reasonable, under the circumstances.

- The other financial institution enters into a contract requiring it to certify annually to the RMLO that it has implemented its AML program, and that it will perform (or its agent will perform) the specified requirements of the RMLO's CIP.

As with any other responsibility performed by a third party, the RMLO is ultimately responsible for that third party's compliance with the requirements of the RMLO's CIP.

Identity Theft Prevention

Introduction and Identity Theft Prevention Program

The Fair Credit Reporting Act's (FCRA) Identity Theft Rules[11] requires RMLOs to develop and implement a written Identity Theft Prevention Program designed to detect red flags of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate its damage. The Program must be appropriate to the size and complexity of the RMLO and the nature and scope of its activities. The Identity Theft Rules is primarily enforced by the Federal Trade Commission (FTC).

The Program must include reasonable policies and procedures to:

a) Identify relevant red flags that apply to each RMLO and incorporate those red flags into its Program;
b) Detect red flags that have been incorporated into the Program of the RMLO;
c) Respond appropriately to any red flags that are detected; and
d) Ensure the Program (including the red flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the RMLO from identity theft.

Each RMLO must provide for the continued administration of the Program and must:

1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;
2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;
3) Train staff, as necessary, to effectively implement the Program; and
4) Exercise appropriate and effective oversight of service provider arrangements.

Appendix A to Part 681

Appendix A to Part 681[12] (Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation) provides guidelines intended to assist financial institutions and creditors

[11] FCRA Identity Theft Rules (16 CFR Part 681)
[12] Appendix A to 16 CFR Part 681

in the formulation and maintenance of a Program that satisfies the requirements of the FCRA Identify Theft Rules.

Below are high level guidelines. Examiners should review Appendix A to Part 681 in its entirety and utilize the **Identity Theft Prevention Exam Procedures** beginning on page 71 when assessing an RMLO's Identity Theft Prevention Program.

Identifying Relevant Red Flags

Red flags are potential patterns, practices, or specific activities indicating the possibility of identity theft. RMLOs should consider the following risk factors in identifying relevant red flags for covered accounts, as appropriate:

1) The types of covered accounts it offers or maintains;
2) The methods it provides to apply for and access a mortgage loan;
3) Its previous experiences with identity theft.

RMLOs should incorporate relevant red flags from sources such as:

1) Incidents of identity theft experienced;
2) Methods of identity theft identified that reflect changes in identity theft risks; and
3) Applicable supervisory guidance.

The Program should include relevant red flags from the following categories, as appropriate. Examples of red flags from each of these categories are appended as Supplement A to Appendix A.

1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
2) The presentation of suspicious documents;
3) The presentation of suspicious personal identifying information, such as a suspicious address change;
4) The unusual use of, or other suspicious activity related to, a covered account; and
5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the RMLO.

Detecting Red Flags

The Program's policies and procedures should address the detection of red flags in connection with the opening of (and existing) covered accounts, such as by:

- **New accounts**: When verifying the identity of the person opening a new account, reasonable procedures may include getting a name, address, and identification number and, for in-person verification, checking a current government-issued identification card, like a driver's license or passport. Refer to **Customer**

Identification Program (CIP) and **Office of Foreign Assets Control (OFAC) Program** sections as these require RMLOs to verify the identity of its customers.

- **Existing accounts:** To detect red flags for existing accounts, the Program may include reasonable procedures to confirm the identity of the person, to monitor transactions, and to verify the validity of change-of-address requests.

Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the red flags the RMLO has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a RMLO should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by RMLO or third party, or notice that a customer has provided information related to a covered account held by the RMLO to someone fraudulently claiming to represent the RMLO or to a fraudulent website. Appropriate responses may include the following:

a) Monitoring a covered account for evidence of identity theft;
b) Contacting the customer;
c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
d) Notifying law enforcement.

Updating the Program

RMLOs should update the Program (including the red flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

a) The experiences of the RMLO with identity theft;
b) Changes in methods of identity theft;
c) Changes in methods to detect, prevent, and mitigate identity theft;
d) Changes in the types of accounts offered; and
e) Changes in the RMLO's business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Methods for Administering the Program

Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

a) Assigning specific responsibility for the Program's implementation;
b) Reviewing reports prepared by staff regarding compliance;
c) Approving material changes to the Program as necessary to address changing identity theft risks; and

d) Oversight of service provider arrangements to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Other Applicable Legal Requirements

In addition to the requirements outlined in the Identity Theft Rules, RMLOs should be mindful of the requirement to file SARs in accordance with applicable law and regulation when fraud and potential suspicious activity is identified.

Supplement A to Appendix A

In addition to incorporating its own red flags, Supplement A under Appendix A to Part 681 provides RMLOs additional examples of red flags for consideration in the areas of:

- Alerts, Notifications or Warnings from a Consumer Reporting Agency;
- Suspicious Documents;
- Suspicious Personal Identifying Information;
- Unusual Use of, or Suspicious Activity Related to, the Covered Account; and
- Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft

Suspicious Activities Applicable to RMLOs

This section highlights potential indicators of suspicious activity related to mortgage fraud and other illicit activity that may impact the mortgage industry. These do not constitute an exhaustive list of common fraud schemes and red flags. The presence of any of these activities may indicate a need for further due diligence and a decision whether to file a SAR. Examiners should use this as general illustrative guidance only.

Mortgage Fraud

RMLOs are typically nonbank institutions who primarily lend money for the purposes of obtaining a mortgage. Most RMLOs do not handle cash transactions or accept deposits. Therefore, RMLOs comply with BSA/AML and SAR reporting requirements differently than their depository counterparts. RMLOs are more likely to file a SAR when they are a target of and identify mortgage fraud schemes. RMLOs may not necessarily be able to detect money laundering activity since money launderers typically integrate illicit funds through regular and timely payments. Between 2017 and August 2019, only 26 percent of SAR filings associated with residential mortgages included money laundering or structuring[13].

[13] FinCEN SAR Stats webpage accessed, and report generated on 9/11/19. 856 of 3,228 SARs filed by "Loan or Finance Company" between 2017 and August 2019 with "Residential Mortgage" as the *Product Type* listed "Money Laundering" and/or "Structuring" as a *Suspicious Activity Category / Type*.

Mortgage fraud is one of the most significant operational risks and forms of suspicious activity facing RMLOs in the ordinary course of business. Instances of mortgage fraud are expected to rise due to a variety of factors, including advances in technology, rising home prices, increased demand for homes, and sophistication of fraudsters[14].

Mortgage fraud generally involves material misrepresentation or omission of information, with the intent to deceive or mislead lenders or homeowners. There are two motivations for mortgage fraud[15]:

- **Fraud for housing:** This type of fraud is typically committed for the primary purpose of purchasing a home. This scheme usually involves a single loan where the borrower provides falsified information (altered pay stubs, W2s, bank statements, tax returns, employment information, etc.). In many cases, the fraud is assisted or initiated by mortgage industry insiders, including brokers, appraisers, closing agents, and RMLOs.

- **Fraud for profit:** This type of fraud is typically committed for the primary purpose of gaining illicit proceeds. Those who commit this type of mortgage fraud are often mortgage industry insiders using their specialized knowledge or authority to commit or facilitate the fraud. Fraud for profit aims not to secure housing but involves multiple loans and elaborate schemes to misuse the mortgage lending process and steal cash and equity from lenders or homeowners. Investigations and reporting indicate a high percentage of mortgage fraud involves collusion by industry insiders, such as banks officers, appraisers, brokers, attorneys, RMLOs, and other professionals engaged in the industry.

The FFIEC[16], FinCEN[17], FBI[18] and Fannie Mae[19] provide detailed analyses of commonly reported mortgage fraud schemes, trends, and potential red flags. Using these resources and implementing an effective BSA/AML Program will allow RMLOs to assist law enforcement efforts against illicit mortgage-related activities, help protect the company and its customers from financial loss and support the housing markets and U.S. financial system as a whole.

As discussed above, there are two primary motivations behind mortgage fraud that can be perpetrated by borrowers, industry insiders or both. When demand for homes is strong and home prices are high, some homebuyers make every attempt necessary to qualify

[14] See CoreLogic 2018 Mortgage Fraud Report (published 9/11/18)
[15] Mortgage Fraud is defined as a material misstatement, misrepresentation, or omission that is relied upon by an underwriter or lender to fund, purchase, or insure a loan. Mortgage fraud is divided into two categories: fraud for property and fraud for profit. FBI Financial Institution/Mortgage Fraud webpage. Additional information on mortgage fraud can be found at www.fincen.gov/mortgage-loan-fraud.
[16] FFIEC BSA/AML Examination Manual: Appendix F – Money Laundering and Terrorist Financing Red Flags
[17] FinCEN Advisory FIN-2012-A009 (issued 8/16/12) – Suspicious Activity Related to Mortgage Loan Fraud
[18] FBI Financial Institution/Mortgage Fraud
[19] Fannie Mae Mortgage Fraud Prevention webpage: Mortgage Fraud Common Red Flags & Fraud Schemes and their Characteristics

for a mortgage loan. According to the 2018 CoreLogic Mortgage Fraud Report[20], undisclosed real estate liabilities, credit repair, questionable down payment sources, and income falsification are the most likely misrepresentations made by these homebuyers.

Still relevant today, the FFIEC Fraud Investigations Symposium published *The Detection and Deterrence of Mortgage Fraud Against Financial Institutions: A White Paper* in 2010 intended to raise the awareness of and assist examiners in identifying various mortgage fraud schemes perpetrated against financial institutions.

FinCEN provides the following examples of commonly used mortgage loan fraud types:

Occupancy fraud	Occurs when borrowers, to obtain favorable loan terms, claim that subject properties will be their primary residences instead of vacation or investment properties. It also occurs when subjects apply for loans for properties that others, such as family members, will actually occupy.
Income fraud	Includes both overstating income (to qualify for larger mortgages) and understating income (to qualify for hardship concessions and modifications).
Appraisal fraud	Includes both overstating home value to obtain more money from a sale of property or cash-out refinancing, and understating home value in connection with a plan to purchase a property at a discount.
Liability fraud	Occurs when borrowers fail to list significant financial liabilities on mortgage loan applications, such as other mortgages, and student or car loans, Without complete liability information, lenders cannot accurately assess borrowers' ability to repay debts.
Employment fraud	Includes misrepresenting whether, where, and for how long borrowers have been employed; whether borrowers are unemployed or collecting unemployment benefits; and whether borrowers are independent contractors or business owners.

An example of employment fraud includes a 2018 fraud alert released by Fannie Mae regarding a three-year trend of fraudulent employers listed on loan applications[21]. The schemes were in California and involved mortgage brokers; however, similar activities occur in other states. According to the fraud alert, a few red flags that correspond with this trend include:

- Employment (occupation) does not "sensibly" coincide with borrower's profile (age or experience);
- Borrower on current job for short period of time;
- Prior borrower employment shows "Student;"
- Starting salary appears high;
- Purported employer does not exist; and
- Gift letters are substantial and are not, or cannot be, verified.

[20] CoreLogic 2018 Mortgage Fraud Report (published 9/11/18)
[21] Fannie Mae's Mortgage Fraud Program Alert: *Misrepresentation of Borrower Employment* (updated 10/16/18)

It is recommended that examiners review the resources below to identify potential mortgage fraud schemes and red flags that may apply to the RMLO and apply these to the overall assessment of the RMLO's BSA/AML Program.

- Fannie Mae Mortgage Fraud Common Red Flags
- Fannie Mae Fraud Schemes and their Characteristics
- FBI Common Mortgage Fraud Schemes
- FFIEC BSA/AML Examination Manual Appendix F: Money Laundering and Terrorist Financing Red Flags
- FinCEN Possible Red Flag Indicators of Mortgage Loan Fraud

*Examiners can also utilize the Fannie Mae Mortgage Fraud Prevention page to identify mortgage fraud trends and watch its *Anti-Fraud Partnership Training Series* that covers tutorials such as: Basics of Mortgage Fraud, Reverse Mortgage Fraud, Short Sale Fraud and Straw Buyers. Freddie Mac provides Quality Control and Fraud resources[22], including fraud mitigation best practices, mortgage fraud prevention and screening processes.

It is important to note that government-sponsored enterprises (GSEs) require RMLOs to comply with BSA and to report instances of mortgage fraud. For example, RMLOs are required to notify Fannie Mae within 30 days if a reasonable basis exists to conclude that any misrepresentation or fraud occurred in connection with the origination or sale of the loan[23]. Freddie Mac requires seller/servicers to meet all guide requirements relating to fraud prevention, detection, and reporting, including Freddie Mac's Exclusionary List and comply with BSA requirements[24]. These GSE compliance and notification requirements are separate from BSA and do not relieve a RMLO of its obligation to file a SAR.

When completing SARs on suspected mortgage loan fraud, RMLOs should indicate the type of mortgage loan fraud by entering the appropriate code in the FinCEN SAR and provide a detailed description in the SAR narrative. For activity that does not have a corresponding code, financial institutions should identify "Other" and describe the activity in the narrative. In addition, RMLOs should include their NMLS Unique Identifier to assist law enforcement in identifying the RMLO as a mortgage company. The FinCEN SAR was updated in 2018 to allow RMLOs to select "*Mortgage (NMLS ID)*" as their form of financial institution identification.

Suspicious Activity Reporting is covered in more detail under **Suspicious Activity Report (SAR) – Reporting Requirements** starting on page 42.

Below are a few examples of common mortgage fraud schemes and potential red flags identified in Fannie Mae, FBI, FFIEC and FinCEN resources.

[22] See Freddie Mac Quality Control and Fraud tab (accessed 9/13/19)
[23] See Fannie Mae Selling Guide *A3-4-03: Preventing, Detecting, and Reporting Mortgage Fraud* (updated 4/3/19)
[24] See Freddie Mac Single-Family Seller/Servicer Guide, *Chapter 3201.2: Fraud and other Suspicious Activity reporting requirements* (updated 4/13/16; accessed 9/13/19)

Examples of Mortgage Fraud Schemes

- ***Straw Buyers Schemes*** include loan applicants used by fraud perpetrators to obtain mortgages and are used to disguise the true buyer or the true nature of the transaction.
- ***Air Loan Schemes*** are loans to a straw or non-existent buyer on a non-existent property.
- ***Double Sale Schemes*** are the sale of one mortgage note to more than one investor.
- ***Property Flipping Schemes*** occurs when property is purchased and resold quickly at an artificially inflated price, using a fraudulently inflated appraisal.
- ***Ponzi, Investment Club, or Chunking Schemes*** involve the sale of properties at artificially inflated prices, pitched as investment opportunities to naïve real estate investors who are promised improbably high returns and low risks.
- ***Builder Bailout/Excessive Sales Incentive Schemes*** are when a seller pays large financial incentives to the buyer and facilitates an inflated loan amount by increasing the sales price, concealing the incentive, and using a fraudulently inflated appraisal.
- ***Equity skimming Schemes*** involve investors using a straw buyer, false income documents, and false credit reports to obtain a mortgage loan in the straw buyer's name. Subsequent to closing, the straw buyer signs the property over to the investor in a quit claim deed, which relinquishes all rights to the property and provides no guaranty to title. The investor does not make any mortgage payments and rents the property until foreclosure takes place months later.
- ***Buy and Bail Schemes*** are when homeowner is current on the mortgage, but the value of the home has fallen below the amount owed, so he or she applies for a purchase money mortgage on another home. After the new property has been secured, the buy and bail borrower will allow the first home to go into foreclosure.
- ***Foreclosure Rescue Schemes*** involve foreclosure "specialists" who promise to help the borrower avoid foreclosure. The borrowers often pay for services that they never receive and, ultimately, lose their homes.
- ***Loan modification Schemes*** are similar to foreclosure rescue scams, and involve perpetrators purporting to assist homeowners who are delinquent in their mortgage payments and are on the verge of losing their home by offering to renegotiate the terms of the homeowners' loan with the lender. The scammers, however, demand large fees up front and often negotiate unfavorable terms for the clients, or do not negotiate at all. Usually, the homeowners ultimately lose their homes.
- ***Short Sale Fraud Schemes*** are when the perpetrator profits by concealing contingent transactions or falsifying material information, including the true value of the property, so the servicer cannot make an informed short sale decision.
- ***Unauthorized Advance Fees and/or Payouts Schemes*** are perpetrated by foreclosure rescue specialists during which fees and/or payouts that were not approved by the servicer agreeing to the short sale are reflected on the Closing Disclosure.
- ***Non-Arm's Length Short Sale Schemes*** involve a fictitious purchase offer made by the homeowner's accomplice (straw buyer) in an attempt to fraudulently reduce the indebtedness on the property and allow the borrower to remain in their home.

- ***Short Sale Flip Schemes*** involve the perpetrator who manipulates the short sale lender into approving a short payoff and conceals an immediate contingent sale to a pre-arranged end buyer at a significantly higher sales price.
- ***Reverse Mortgage Fraud Schemes*** include the perpetrator who manipulates a senior citizen into obtaining a reverse mortgage loan and then pockets the senior victim's reverse mortgage loan proceeds.
- ***Affinity Fraud Schemes*** involve perpetrators who rely on a common bond and exploit the trust and friendship that typically exist in the group of individuals with a common bond to support the scheme. Certain ethnic, religious, professional, or age-related groups are targeted.
- ***Reverse Occupancy Fraud Schemes*** involve a borrower who buys a home as an investment property and lists rent proceeds as income to qualify for the mortgage. But then instead of renting the home, the borrower occupies the home as a primary residence.

Examples of Mortgage Fraud Red Flags

- Borrower/buyer submits invalid documents in order to cancel his or her mortgage obligations or to pay off his or her loan balance(s).
- Borrower/buyer applies for a loan for a "primary residence" but does not reside in the new primary residence as indicated on the loan application; other individuals occupy the borrower/buyer's new primary residence indicating the property is being used as a secondary residence or income-generating property.
- Documents appear to be altered.
- Suspicious credit report issues are identified. Examples include liabilities shown on credit report that are not on mortgage application, length of established credit is not consistent with applicant's age, credit patterns are inconsistent with income and lifestyle, social security number, death, or fraud alerts
- Borrower/buyer requests refinancing for "primary residence" when public and personal documents indicate that the borrower/buyer resides somewhere other than the address on the loan application.
- Low appraisal values, non-arm's length relationships between short sale buyers and sellers, or previous fraudulent sale attempts in short-sale transactions.
- Past misrepresentations made by borrower/buyer in attempts to secure funding, property, refinance, and/or shorts sales.
- Improper/incomplete file documentation, including borrower/buyer reluctance to provide more information and/or unfulfilled promises to provide more information.
- Borrower/buyer attempts to structure currency deposits/withdrawals, or otherwise to hide or disguise the true value of assets, in order to qualify for loan modification programs intended for those homeowners in financial distress.
- Request from third party affiliates on behalf of distressed homeowners to pay fees in advance of the homeowner receiving mortgage counseling, foreclosure avoidance, a loan modification, or other related services.
- Mortgage Application:
    - Significant or contradictory changes from handwritten to typed application;
    - Unsigned or undated application;

- Employer's address shown only as a post office box;
- Loan purpose is cash-out refinance on a recently acquired property;
- Buyer currently resides in subject property;
- Extreme payment shock may signal straw buyer and/or or inflated income;
- Purchaser of investment property does not own residence.

Home Equity Conversion Mortgage (HECM) Program Fraud Schemes

FinCEN issued an advisory regarding fraud schemes related to the Federal Housing Administration (FHA) Home Equity Conversion Mortgage (HECM) program[25]. Below are potential indicators of schemes involving the HECM program based upon general typologies received from law enforcement and HUD officials.

- **Cross Selling:** Involves the theft of a senior's HECM loan proceeds through cross selling of financial products. As a part of this scheme, an individual convinces the senior to use HECM loan proceeds to finance the purchase of expensive and unnecessary insurance, annuities, or other financial products.
- **Cash-out Theft:** Involves the theft of reverse mortgage proceeds by individuals trusted by the senior, including family members, care takers, and RMLOs. For example, a senior may receive a HECM cash-out check and provide the check to the RMLO (or other trusted party). The RMLO or other trusted party then co-endorses the check and deposits it to their business or personal bank account. The senior is instructed to request cash withdrawals directly from the RMLO or another trusted individual. After the senior obtains several withdrawals, he or she is told all the HECM loan proceeds have been received. The RMLO or other trusted party pockets the remaining funds.
- **Straw Owner-Property Flipping:** Involves a "straw buyer" transferring ownership of a typically low-value or problem property to an unsuspecting senior ("straw senior") without going through a mortgage sale. Fraudsters then instruct the straw senior to complete paperwork for a HECM loan against the property, using an overstated appraisal, or assume the identity of the senior to do so themselves. Investigators have noted appraisals as high as 1,000% of the actual fair market value of the home.
- **Straw Owner-Fake Down Payments:** Involves fraudsters "selling" low-value properties to seniors. Using bogus gifts or fraudulent paperwork, fraudsters create the appearance of a large down payment by the senior to purchase the property. The senior is then instructed to take out a HECM loan on the existing home, based on an overstated appraisal, to complete the purchase of the low-value property.
- **Distressed Non-senior Mortgagors:** Distressed mortgagors under the age of 62 will sometimes ask senior parents, other family members, or friends to take a HECM loan for them. In some cases, distressed mortgagors will submit fraudulent paperwork to take out the loan and receive the HECM loan proceeds directly.

[25] FinCEN *Updated Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Loan Modification/Foreclosure Rescue Scams* (issued 6/17/10)

Fraudsters also may assume the identity of a senior victim and take out a HECM loan without the senior's knowledge.

- **Power of Attorney:** In a variety of the fraud schemes noted above, the perpetrator may use a power of attorney (POA) for the senior to apply for and close HECM loans without the full knowledge or participation of the victim. A POA also may be used for either the seller or the buyer in a HECM for Purchase transaction. In many HECM for Purchase schemes, fraudsters purchase properties from homeowners without formally recording the purchase. Instead, the fraudster receives a POA from the homeowner and then "sells" the home to the straw senior using the HECM for Purchase program.

The specific term "HECM" should be included within the narrative portions of all relevant SAR filings and highlight the exact dollar amount(s) associated with the HECM loan proceeds. In addition, if RMLO become aware of any other type of FHA-insured mortgage fraud, FinCEN requests the term "FHA" be included within the narrative portions of the relevant SAR filings.

Marijuana-Related Businesses and Employees

FinCEN issued guidance to clarify BSA expectations for financial institutions seeking to provide services to marijuana-related businesses, which includes individuals who work for and receive compensation from marijuana-related businesses[26]. Among the guidance, a financial institution that decides to provide financial services to a marijuana-related business is required to file a SAR specific to the transaction, irrelevant on any state law that legalizes marijuana-related activity.

Because federal law prohibits the distribution and sale of marijuana, financial transactions involving a marijuana-related business would generally involve funds derived from illegal activity. Therefore, a financial institution is required to file a SAR on activity involving a marijuana-related business (including those duly licensed under state law), in accordance with this guidance and FinCEN's suspicious activity reporting requirements.

The FinCEN guidance also clarifies how financial institutions can provide services to marijuana-related businesses consistent with their BSA obligations. In general, the decision to open, close, or refuse any particular account or relationship should be made by each financial institution based on a number of factors specific to that institution. These factors may include its particular business objectives, an evaluation of the risks associated with offering a particular product or service, and its capacity to manage those risks effectively.

In assessing the risk of providing services to a marijuana-related business and associated individuals, a financial institution should conduct customer due diligence that includes, at a minimum, verifying with the appropriate state authorities whether the business is duly licensed and registered and reviewing the license application (and related documentation)

[26] FinCEN Advisory: *BSA Expectations Regarding Marijuana-Related Businesses* (issued 2/14/14)

submitted by the business for obtaining a state license to operate its marijuana-related business.

As part of its customer due diligence, a financial institution should consider whether a marijuana-related business implicates one of the Cole Memo priorities or violates state law. This is a particularly important factor for a financial institution to consider when assessing the risk of providing financial services to a marijuana-related business. Considering this factor also enables the financial institution to provide information in BSA reports pertinent to law enforcement's priorities. A financial institution that decides to provide financial services to a marijuana-related business or employees are required to file SARs as described below.

One of the BSA's purposes is to require financial institutions to file reports that are highly useful in criminal investigations and proceedings. The guidance below furthers this objective by assisting financial institutions in determining how to file a SAR that facilitates law enforcement's access to information pertinent to a priority.

"Marijuana Limited" SAR Filings

- A financial institution providing financial services to a marijuana-related business that it reasonably believes, based on its customer due diligence, does not implicate one of the Cole Memo priorities or violate state law should file a "Marijuana Limited" SAR.
- The content of this SAR should be limited to the following information: (i) identifying information of the subject and related parties; (ii) addresses of the subject and related parties; (iii) the fact that the filing institution is filing the SAR solely because the subject is engaged in a marijuana-related business; and (iv) the fact that no additional suspicious activity has been identified.
- Use the term "MARIJUANA LIMITED" in the narrative section.

"Marijuana Priority" SAR Filings

- The content of this SAR should include comprehensive detail in accordance with existing regulations and guidance. Details particularly relevant to law enforcement in this context include: (i) identifying information of the subject and related parties; (ii) addresses of the subject and related parties; (iii) details regarding the enforcement priorities the financial institution believes have been implicated; and (iv) dates, amounts, and other relevant details of financial transactions involved in the suspicious activity.
- Financial institutions should use the term "MARIJUANA PRIORITY" in the narrative section to help law enforcement distinguish these SARs.
- A financial institution filing a SAR on a marijuana-related business that it reasonably believes, based on its customer due diligence, implicates one of the Cole Memo priorities or violates state law should file a "Marijuana Priority" SAR.

"Marijuana Termination" SAR Filings

- If a financial institution deems it necessary to terminate a relationship with a marijuana-related business in order to maintain an effective anti-money laundering compliance program, it should file a SAR and note in the narrative the basis for the termination.
- Use the term "MARIJUANA TERMINATION" in the narrative section.
- To the extent the financial institution becomes aware that the marijuana-related business seeks to move to a second financial institution, FinCEN urges the first institution to use Section 314(b) voluntary information sharing (if it qualifies) to alert the second financial institution of potential illegal activity.

Examiners should review the FinCEN Advisory FIN-2014-G001, "*BSA Expectations Regarding Marijuana-Related Businesses"* that details more information on BSA reporting requirements and provides red flags to distinguish priority SARs.

Elder Financial Exploitation

FinCEN issued guidance to assist the financial industry in reporting instances of financial exploitation of the elderly, a form of elder abuse[27]. The "*Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults"*[28] states that elder abuse includes the illegal or improper use of an older adult's funds, property, or assets. Older adults can become targets of financial exploitation by family members, caregivers, scam artists, financial advisers, home repair contractors, fiduciaries (such as agents under power of attorney and guardians), and others. Older adults are attractive targets because they may have significant assets or equity in their homes. They may be especially vulnerable due to isolation, cognitive decline, physical disability, health problems, and/or the recent loss of a partner, family member, or friend. While anyone can be a victim of a financial crime such as identity theft, embezzlement, and fraudulent schemes, certain elderly individuals may be particularly vulnerable.

RMLOs can play a key role in identifying elder financial exploitation during the mortgage loan application process. In addition to filing a SAR, prompt reporting of suspected financial exploitation to adult protective services, law enforcement, and/or long-term care ombudsmen can trigger appropriate intervention, prevention of financial losses, and other remedies.

RMLOs should evaluate indicators of potential financial exploitation in combination with red flags and expected transaction activity being conducted by or on behalf of the elder. Additional investigation and analysis may be necessary to determine if the activity is suspicious.

SARs are a valuable avenue for RMLOs to report elder financial exploitation. Consistent with the standard for reporting suspicious activity, if a RMLO knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the RMLO knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, the RMLO should file a SAR.

In order to assist law enforcement in its effort to target instances of financial exploitation of the elderly, FinCEN requests that financial institutions select the appropriate characterization of suspicious activity in the Suspicious Activity Information section of the SAR form and include the term "elder financial exploitation" in the narrative portion of all relevant SARs filed. The narrative should also include an explanation of why the institution

[27] FinCEN *Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation* (issued 2/22/11)
[28] *Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults* (issued 9/24/13)

knows, suspects, or has reason to suspect that the activity is suspicious. It is important to note that the potential victim of elder financial exploitation should not be reported as the subject of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.

CFPB Guidance on Reporting Suspected Elder Financial Exploitation

The CFPB issued an advisory in July 2019 titled, *"Reporting of Suspected Elder Financial Exploitation by Financial Institutions"*[29] which is an update to its 2016 advisory, urging financial institutions to report to the appropriate local, state and federal authorities whenever they suspect that an older adult is the target or victim of elder financial exploitation (EFE), in addition to filing SARs. The CFPB provides six categories of best practices to help financial institutions prevent elder financial abuse and intervene effectively when it occurs:

1. Developing and implementing internal protocols and procedures for protecting account holders from elder financial exploitation;
2. Training management and staff to prevent, detect, and respond to suspicious events
3. Detecting elder financial exploitation by harnessing technology;
4. Reporting all cases of suspected exploitation to relevant federal, state and local authorities;
5. Protecting older account holders by complying with the Electronic Fund Transfer Act (EFTA) and Regulation E and by offering age-friendly services that can enhance protections against financial exploitation;
6. Collaborating with other stakeholders such as law enforcement, adult protective services, and service organizations.

In February 2019, the CFPB published a research report, *"Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends"* where it analyzed SARs filed by a financial institution from 2013 to 2017 regarding suspected EFE[30]. The CFPB found that SAR filings on elder financial exploitation quadrupled from 2013 to 2017. In 2017 alone, financial institutions filed 63,500 SARs reporting elder financial abuse, but the CFPB states that this likely represents only a tiny fraction of the actual 3.5 million incidents of elder financial exploitation estimated to have happened in 2017.

The CFPB also found that while financial institutions are increasingly filing elder financial exploitation SARs, they often do not indicate that they reported the suspicious activity directly to first responders. Fewer than one-third (28 percent) of elder financial exploitation SARs specify that the financial institution reported the activity to adult protective services,

[29] CFPB *Reporting of Suspected Elder Financial Exploitation by Financial Institutions*: An update to the 2016 Advisory and Recommendations for Financial Institutions on Preventing and Responding to Elder Financial Exploitation (issued 7/17/19)
[30] CFPB *Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends* (issued 2/27/19)

law enforcement, or other authorities. If the financial institution is not reporting to these authorities, this is a missed opportunity to strengthen prevention and response.

The CFPB emphasizes the importance of reporting EFE to the relevant authorities in addition to filing SARs. More reporting to the relevant law enforcement agencies can increase investigation, prosecution, and the likelihood that victims will receive appropriate services. The CFPB pointed to FINCEN guidance[31] advising financial institutions to provide SAR information and supporting documentation to authorized investigatory agencies: *"Financial institutions must provide all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency." "Disclosure of SARs to appropriate law enforcement and supervisory agencies is protected by the safe harbor provisions applicable to both voluntary and mandatory suspicious activity reporting by financial institutions."*

In addition, it is important to note that *"Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults"* provides guidance to financial institutions clarifying that reporting suspected financial abuse of older adults to appropriate local, state, or federal agencies does not, in general, violate the privacy provisions of the Gramm-Leach-Bliley Act (GLBA) or its implementing regulations. In fact, specific privacy provisions of the GLBA and its implementing regulations permit the sharing of this type of information under appropriate circumstances without complying with notice and opt-out requirements[32].

In its July 2019 report the CFPB highlighted 26 states (plus the District of Columbia) that mandate reporting of suspected EFE by financial institutions or financial professionals. Examiners should review state-specific laws applicable to financial institution reporting requirements regarding elder financial exploitation and incorporate any requirements in their examination. The CFPB provides these state-specific reporting requirements as Appendices in its report.

OFAC Sanctions Lists Matches

FinCEN provided interpretive guidance[33] stating that a financial institution that files a blocking report with OFAC due to the involvement in a transaction or account of a person designated as a Specially Designated Global Terrorist, a Specially Designated Terrorist, a Foreign Terrorist Organization, a Specially Designated Narcotics Trafficker Kingpin, or a Specially Designated Narcotics Trafficker, is deemed to have concurrently filed a SAR.

The interpretation does not affect a RMLO's obligation to identify and report suspicious activity beyond the fact of the OFAC match. To the extent that a RMLO is in possession

[31] FinCEN Guidance: *Suspicious Activity Report Supporting Documentation* (issued 6/13/07)
[32] See *Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults* (issued 9/24/13)
[33] FinCEN Guidance: *Interpretation of Suspicious Activity Reporting Requirements to Permit the Unitary Filing of Suspicious Activity and Blocking Reports* (issued 12/04)

of information not included on the blocking report filed with OFAC, a separate SAR should be filed with FinCEN including that information.

The interpretation also does not affect a RMLO's obligation to file a SAR even if it has filed a blocking report with OFAC, to the extent that the facts and circumstances surrounding the OFAC match are independently suspicious and are otherwise required to be reported under existing FinCEN regulations. In those cases, the OFAC blocking report would not satisfy a RMLO's SAR filing obligation.

Further, nothing in the interpretation is intended to preclude a RMLO from filing a SAR to disclose additional information concerning the OFAC match, nor does it preclude a RMLO from filing a SAR if it has reason to believe that terrorism or drug trafficking is taking place, even though there is no OFAC match.

Finally, the interpretation does not apply to blocking reports filed to report transactions and accounts involving persons owned by, or who are nationals of, countries subject to OFAC-administered sanctions programs. Such transactions should be reported on SARs under the suspicious activity reporting rules if, and only, if, the activity itself appears to be suspicious under the criteria established by the suspicious activity reporting rules.

Email Compromise Fraud

FinCEN issued an advisory to help financial institutions guard against a growing number of email fraud schemes in which criminals misappropriate funds by deceiving financial institutions and their customers into conducting wire transfers[34]. The advisory also provides red flags that were developed in consultation with FBI and Secret Service to help financial institutions identify and prevent such -mail fraud schemes.

FinCEN issued an updated advisory in July 2019[35] providing important updates that may assist financial institutions in detecting, preventing, and reporting e-mail compromise fraud and associated money laundering activity.

Email compromise fraud includes schemes in which:

1) Criminals compromise the email accounts of victims to send fraudulent payment instructions to financial institutions or other business associates in order to misappropriate funds or value; or
2) Criminals compromise the email accounts of victims to effect fraudulent transmission of data that can be used to conduct financial fraud. The main types of email compromise include:
    - ***Business Email Compromise (BEC):*** Targets accounts of financial institutions or customers of financial institutions that are operational entities, including commercial, non-profit, nongovernmental, or government entities.

[34] FinCEN *Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes* (issued 9/9/16)
[35] FinCEN *Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes* (issued 7/16/19)

- ***Email Account Compromise (EAC):*** Targets personal email accounts belonging to an individual.

While the U.S. government and industry are heavily engaged in efforts to prevent email compromise fraud, reported incidents and aggregate attempted fraudulent wire amounts continue to rise. For example, the FBI reported over $12 billion in potential losses domestically and internationally from October 2013 to May 2018 from email compromise fraud. Since the 2016 advisory was issued, FinCEN has received over 32,000 reports involving almost $9 billion in attempted theft from BEC fraud schemes affecting U.S. financial institutions and their customers[36]. This represents a significant economic impact on the businesses, individuals, and governments that are targeted by these schemes.

According to FinCEN, real estate transactions have been a particularly lucrative target for BEC schemes. The large dollar volumes involved in such transactions, whether for down payments on a property or the final transfer of proceeds upon closing, are an attractive target of opportunity for criminals engaged in BEC activity. FinCEN analysis reveals that BEC criminals often targeted several potential vulnerabilities of common real estate-related business processes:

a) Readily available detailed public information regarding potential real estate transactions and counterparties (e.g., real estate agents and homeowners);
b) General communication of transactions between real estate counterparties conducted via email; and
c) A common lack of strong authentication processes for verifying identity and validity of instructions in associated communications.

FinCEN encourages financial institutions and their customers to assess the vulnerability of their business processes to compromise and consider if there are appropriate steps within their risk management approach to "harden" or increase the resiliency of their processes and systems against email fraud schemes. This can include considering the risk surrounding the its business processes and practices to 1) authenticate participants in communications, 2) authorize transactions, and 3) communicate information and changes about transactions.

Overall, financial institutions have provided valuable reporting to FinCEN regarding the nature and victims of email compromise schemes. While the recovery of BEC stolen funds is not assured, FinCEN has had greater success in recovering funds when victims or financial institutions report BEC-unauthorized wire transfers to law enforcement within 24 hours. In September 2018, the FBI's Internet Crime Complaint Center's Recovery Asset Team (RAT) received a complaint filed by a BEC victim located in Colorado. The victim reported that they initiated a fraudulent wire transfer of $56,179.27 after receiving a spoofed email from a lending agent during a real estate transaction. The RAT contacted the victim's bank and worked with the fraud department to freeze the funds. The victim

[36] FBI Alert I-071218-PSA: *Business E-mail Compromise the 12 Billion Dollar Scam* (issued 7/12/18)

was able to recover $54,000 of the funds and purchase their new home[37].

With respect to email compromise fraud involving fraudulent payment instructions, a financial institution has a SAR filing obligation regardless of whether the scheme or involved transactions were successful, and regardless of whether the financial institution or its customers incurred an actual loss.

When filing a SAR regarding suspicious transactions that involve cyber-events (such as BEC fraud), financial institutions should provide all pertinent available information on the event and associated suspicious activity, including cyber-related information, in the SAR form and narrative[38]. FinCEN requests that financial institutions reference FinCEN Advisory FIN-2019-A005 and include the following key terms in the SAR narrative:

- "BEC FRAUD" when businesses or organizations are the scheme victims
- "EAC FRAUD" when individuals are the scheme victims

Financial institutions should also select SAR field 42 (*Cyber event*) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and possible BEC or EAC fraud. Financial institutions should include one or both key terms to the extent they are able to distinguish between BEC and EAC fraud. Additionally, financial institutions should include any relevant technical cyber indicators related to the email compromise fraud and associated transactions within the available structured cyber event indicator SAR fields 44(a)-(j), (z).

For additional information regarding typologies and red flags of email compromise schemes in Suspicious Activity Reports (SARs), examiners should review FinCEN Advisory FIN-2016-A003, *"Advisory to Financial Institutions on Email Compromise."*

For additional information regarding SAR reporting requirements specific to email compromise schemes, examiners should review FinCEN Advisory FIN-2019-A005, *"Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes."*

Cyber Events

FinCEN issued an advisory in October 2016 to assist financial institutions in understanding BSA obligations regarding cyber-events and cyber-enabled crime and to highlight how BSA reporting helps U.S. authorities combat cyber-events and cyber-enabled crime[39]. For the purpose of this advisory:

- **Cyber-Event:** An attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information.

[37] FBI 2018 Internet Crime Report (issued 4/22/19)
[38] FinCEN *FAQs regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through SARs* (issued 10/25/16)
[39] FinCEN *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime* (issued 10/25/16)

- **Cyber-Enabled Crime:** Illegal activities (e.g., fraud, money laundering, identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers.
- **Cyber-Related Information:** Information that describes technical details of electronic activity and behavior, such as IP addresses, timestamps, and Indicators of Compromise (IOCs). Cyber-related information also includes, but is not limited to, data regarding the digital footprint of individuals and their behavior.

The size, reach, speed, and accessibility of the U.S. financial system make financial institutions attractive targets to traditional criminals, cybercriminals, terrorists, and state actors. These actors target financial institutions' websites, systems, and employees to steal customer and commercial credentials and proprietary information; defraud financial institutions and their customers; or disrupt business functions. Financial institutions play an important role in safeguarding customers and the financial system from these threats through timely and thorough reporting of cyber-events and cyber-related information in SARs. In response, FinCEN encourages financial institutions to incorporate cyber-related information into their BSA/AML monitoring efforts and report relevant cyber-related information in SARs.

Additionally, financial institutions are encouraged to internally share relevant information across the organization, including BSA/AML staff, cybersecurity staff, risk management teams, and other affected departments. Information sharing across the organization helps identify suspicious activity and criminal actors, develop a better understanding of BSA/AML risk exposure, and provides for more comprehensive and complete SAR reporting.

FinCEN and law enforcement regularly use information financial institutions report under the BSA to initiate investigations, identify criminals, and disrupt and dismantle criminal networks. The cyber-related information that financial institutions include in this reporting is a valuable source of investigatory leads. Law enforcement has been able to use cyber-related information reported to track criminals, identify victims, and trace illicit funds.

According to FinCEN, if a financial institution knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions, it should be considered part of an attempt to conduct a suspicious transaction or series of transactions. Cyber-events targeting financial institutions that could affect a transaction or series of transactions would be reportable as suspicious transactions because they are unauthorized, relevant to a possible violation of law or regulation, and regularly involve efforts to acquire funds through illegal activities.

In determining whether a cyber-event should be reported, a financial institution should consider all available information surrounding the cyber-event, including its nature and the information and systems targeted. Similarly, to determine monetary amounts involved in the transactions or attempted transactions, a financial institution should consider in aggregate the funds and assets involved in or put at risk by the cyber-event. Regardless

as to whether a SAR is required, FinCEN encourages financial institutions to report *any* egregious, significant, or damaging cyber-events and cyber-enabled crime.

When filing a mandatory or voluntary SAR involving a cyber-event, financial institutions should provide complete and accurate information, including relevant facts in appropriate SAR fields, and information about the cyber-event in the narrative section of the SAR in addition to any other related suspicious activity. As needed, financial institutions may also attach a comma separated value (CSV) file to SARs to report data, such as cyber-event data and transaction details, in tabular form.

FinCEN provides illustrative examples of cyber-events in which SAR reporting is required in its advisory and detailed FAQs to supplement its advisory on cyber-events and cyber-enabled crime to assist financial institutions in reporting cyber-events and cyber-enabled crime through SARs. Examiners are encouraged to review both for more information:

- FinCEN Advisory FIN-2016-A005
- FinCEN FAQs on Cyber-Events

Suspicious Activity Report (SAR) – Reporting Requirements

Introduction

A RMLO is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the RMLO:

- Involves funds derived from illegal activity;
- Attempts to disguise funds derived from illegal activity;
- Is designed to evade regulations promulgated under the BSA;
- Lacks a business or apparent lawful purpose; or
- Involves the use of the RMLO to facilitate criminal activity[40].

The mortgage industry does not typically deal in large cash transactions or take deposits, so traditional money-laundering schemes will not affect many RMLOs. Additionally, since RMLOs are not defined as a "financial institution" under 31 CFR §1010.100, they are not currently required to file Currency Transaction Reports (CTRs) or many of the other reports that are required of businesses defined as a "financial institution."[41]

However, RMLOs are required to file a SAR if it receives a cash payment of $5,000 or more and knows, suspects, or has reason to suspect the cash payment involves illegal or suspicious activity (i.e. the individual cannot verify the source of the cash payment). Additionally, RMLOs are required to file Form 8300 if it receives any cash payment over $10,000 – see **IRS Form 8300** below for more information.

[40] 31 CFR §1029.320 – Reports by loan or finance companies of suspicious transactions.
[41] FinCEN *Important Notice to Non-Bank Residential Mortgage Lenders and Originators* (issued 8/13/12)

RMLOs file all SARs electronically through the BSA Electronic Filing (E-Filing) System. The BSA E-Filing system supports electronic filing of BSA forms through a FinCEN secure network. It also allows RMLOs to send and receive secure messages to and from FinCEN. Additionally, FinCEN uses the system to issue advisories and system updates to the user community.

RMLOs must register with FinCEN through the BSA E-Filing System before filing any SARs. Registration includes providing a point-of-contact that serves as a liaison between BSA E-Filing and the RMLO. This individual is typically the designated BSA/AML Compliance Officer. Depending on the size, risk level, and BSA/AML staffing, a RMLO may have one or multiple user accounts within the institution's BSA E-Filing account who are responsible for filing SARs on its behalf.

FinCEN provides detailed guidance on SAR reporting requirements as frequently asked questions (FAQs). In addition to the guidance below (extracted from the FFIEC BSA/AML Examination Manual), examiners are encouraged to review the FAQs and 31 CFR §1029.320 for more information on SAR reporting requirements applicable to RMLOs.

Reporting Requirements

RMLOs are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing, and certain other crimes above prescribed dollar thresholds. When evaluating suspicious activity and completing the SAR, RMLOs should, to the best of their ability, identify the characteristics of the suspicious activity. *Suspicious Activity Information, Part II* of the SAR provides a number of categories with different types of suspicious activity. Within each category, there is the option of selecting "Other: if none of the suspicious activities apply. However, the use of "Other" should be limited to situations that cannot be broadly identified within the categories provided[42].

After thorough research and analysis has been completed, findings are typically forwarded to a final decision maker, who is typically the designated BSA Compliance Officer or a BSA/AML committee. The RMLO should have policies, procedures, and processes for referring unusual activity from all business lines to the personnel responsible for evaluating unusual activity. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation. The decision maker, whether an individual or committee, should have the authority to make the final SAR filing decision – See **Systems to Identify, Research, and Report Suspicious Activity** for more information.

RMLOs should document SAR decisions, including the specific reason for filing or not filing a SAR. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR.

[42] FFIEC BSA/AML Examination Manual: Suspicious Activity Reporting – Overview (accessed 9/12/19)

The decision to file a SAR is an inherently subjective judgment. Examiners should focus on whether the RMLO has an effective SAR decision-making process, not individual SAR decisions. Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process. In those instances where the RMLO has an established SAR decision-making process, has followed existing policies, procedures, and processes, and has determined not to file a SAR, the RMLO should not be penalized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith[43].

IRS Form 8300

To the extent a RMLO receives more than $10,000 in cash, it must file Form 8300 with the Internal Revenue Service (IRS) and FinCEN within 15 days after the transaction occurs. Specifically:

- If the initial payment exceeds $10,000, the RMLO must report the initial payment within 15 days of its receipt.
- If the initial payment does not exceed $10,000, the RMLO must aggregate the initial payment and subsequent payments made within one year of the initial payment until the aggregate amount exceeds $10,000, and report with respect to the aggregate amount within 15 days after receiving the payment that causes the aggregate amount to exceed $10,000[44].

IRS Form 8300 provides valuable information to assist the Internal Revenue Service, FinCEN, and law enforcement in its anti-money laundering efforts. When businesses comply with the reporting laws, they provide authorities with an audit trail to investigate possible tax evasion, drug dealing, terrorist financing and other criminal activities.

In addition to filing Form 8300 with the IRS, RMLOs are required to furnish a written statement to each person whose name is required to be included in the Form 8300 by January 31 of the year that immediately follows the year the customer made the cash payment. This statement must include the name, address, contact person, and telephone number of the business filing Form 8300, the aggregate amount of reportable cash the business was required to report to the IRS from the person receiving the statement, and that the business provided this information to the IRS.

A good example of a situation that would require a RMLO to file Form 8300 is if a borrower brings $10,000 in cash to the closing table. This example highlights the importance of RMLOs developing comprehensive BSA/AML policies, procedures, and controls specific to departments and business channels. It is prudent for all personnel to understand BSA reporting requirements and when to report suspicious activity – in this case closers.

[43] Refer to FFIEC BSA/AML Examination Manual: Appendix R *Interagency Enforcement Statement* for additional information.
[44] See 31 CFR §1010.330

RMLOs file Form 8300 electronically through the BSA E-Filing System. RMLOs are required to retain a copy of every Form 8300 filed and the required statement it sends for five years from the date filed.

For information, examiners can review the IRS Form 8300 Reference Guide.

Foreign Bank and Financial Accounts Reporting (FBAR)

The BSA gave the Department of Treasury authority to collect information from any U.S. person or entity who has financial interests in or signature authority over financial accounts maintained with financial institutions located outside of the United States. This provision of the BSA requires that a FinCEN Form 114 (FBAR) be filed if the aggregate maximum values of the foreign financial accounts exceed $10,000 at any time during the calendar year.

The FBAR is required because foreign financial institutions may not be subject to the same reporting requirements as domestic financial institutions. The FBAR is also a tool used by the U.S. government to identify persons who may be using foreign financial accounts to circumvent U.S. law. Information contained in FBARs can be used to identify or trace funds used for illicit purposes or to identify unreported income maintained or generated abroad.

As with SARs and Form 8300, the FBAR is filed electronically using the BSA E-Filing System. Companies must keep records for each account required to be reported on an FBAR that includes the name on the account, account number, name and address of the foreign bank, type of account, and maximum value during the year. These records must be maintained for five years from the due date of the FBAR.

For information, examiners can review the IRS FBAR Resource Page.

Timing of a SAR Filing

The SAR rules require that a SAR be electronically filed through the BSA E-Filing System no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect is identified on the date initial detection, the time period for filing a SAR may be extended an additional 30 calendar days to identify a suspect, but in no case can reporting be delayed more than 60 calendar days after the date of the initial detection.

The time period for filing a SAR starts when the RMLO, 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. The 30-day (or 60-day) period

does not begin until an appropriate review is conducted, and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR regulation[45].

In situations involving violations that require immediate attention, such as suspected terrorist financing or ongoing money laundering schemes, in addition to filing a timely SAR, a RMLO must immediately notify, by telephone, an "appropriate law enforcement authority" and the RMLO's primary regulator. Notifying law enforcement of a suspicious activity does not relieve a RMLO of its obligation to file a SAR.

SAR Quality

RMLOs are required to file SARs that are complete, thorough, and timely. Inaccurate information on the SAR, or an incomplete or disorganized narrative, may make further analysis difficult, if not impossible. However, there may be legitimate reasons why certain information may not be provided in a SAR, such as when the filer does not have the information. A thorough and complete narrative may make the difference in determining whether the described conduct and its possible criminal nature are clearly understood by law enforcement. Because the SAR narrative section is the only area summarizing suspicious activity, the section, as stated on the SAR, is "critical." Thus, a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

By their nature, SAR narratives are subjective, and examiners generally should not criticize the RMLO's interpretation of the facts. Nevertheless, RMLOs should ensure that SAR narratives are complete, thoroughly describe the extent and nature of the suspicious activity and are included within the SAR. In general, a SAR narrative should identify the five essential elements of information (who? what? when? where? and why?) for the suspicious activity being reported. The method of operation (or how?) is also important and should be included in the narrative. As stated in **Suspicious Activities Applicable to RMLOs**, the FinCEN SAR Electronic Filing Requirements allows RMLOs to select "Mortgage (NMLS ID)" as their form of financial institution identification.

The FFIEC BSA/AML Examination Manual includes additional guidance in Appendix L: SAR Quality Guidance to assist RMLOs in drafting SARs and to assist examiners in evaluating SAR narratives. In addition, each FinCEN advisory described above specific to mortgage fraud, marijuana-related businesses, email compromise schemes, cyber events, and others include guidance and recommendations on SAR reporting. Visit the FinCEN Advisory page for more information.

Record Retention and Supporting Documentation

RMLOs must retain copies of SARs and the original (or business record equivalent) of any supporting documentation concerning any SAR that is filed, for a period of five years

[45] Bank Secrecy Act Advisory Group "Section 5 – Issues and Guidance," *The SAR Activity Review – Trends, Tips & Issues* (issued 5/2006), page 44. For examples of when the date of initial detection occurs, refer to *SAR Activity Review – Trends, Tips, and Issues* (issued 10/2008), page 38.

from the date of filing the SAR. RMLOs must make all supporting documentation available to FinCEN, or any federal, state, or local law enforcement agency authorized to examine the RMLO for compliance with the Bank Secrecy Act.

Prohibition of SAR Disclosure

No RMLO, director, officer, employee, or agent of the institution that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. A SAR and any information that would reveal the existence of a SAR, are confidential, except as is necessary to fulfill BSA obligations and responsibilities. For example, the existence or even the non-existence of a SAR must be kept confidential, as well as the information contained in the SAR to the extent that the information would reveal the existence of a SAR.

This may be difficult for RMLOs who are required by law to take "adverse action" against a mortgage loan applicant. The RMLO must take caution when taking "adverse action" and selecting appropriate reason(s) for denial when the main reason involves suspicion of fraud, to ensure that the applicant is not made aware of the existence of a SAR. Examiners should review the RMLO's policies, procedures, and processes that address these situations and review sample loans that were denied due to suspicion of fraud. Examiners should not criticize the adverse action or reason(s) for denial if the RMLO has a consistent, written process for documenting these situations and makes every effort comply with BSA requirements.

Provided that no person involved in any reported suspicious transaction is notified that the transaction has been reported, the RMLO can provide a SAR, or any information that would reveal the existence of a SAR, to FinCEN and any federal, state, or local law enforcement agency that has the authority to examine the RMLO for compliance with the Bank Secrecy Act[46].

Information Sharing

Section 314 of the USA PATRIOT Act, implemented on September 26, 2002, established procedures for information sharing to deter money laundering and terrorist activity. On February 5, 2010, FinCEN amended its regulations under 31 CFR 1010.540 to allow state, local, and certain foreign law enforcement agencies access to the information sharing program.

Information Sharing Between Law Enforcement and Financial Institutions – Section 314(a) of the USA PATRIOT Act

A federal, state, local, or foreign law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on its behalf, certain information from a financial institution. Upon receiving a completed written certification from a law

[46] See 31 CFR §1029.320(d)(1)(ii)(A)(1)

enforcement agency, FinCEN may require a financial institution 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.

Upon receiving an information request, a financial institution must conduct a one-time search of its records to identify accounts or transactions of a named suspect. Unless otherwise instructed by an information request, financial institutions must search their records 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. The financial institution must search its records and report any positive matches to FinCEN within 14 days, unless otherwise specified in the information request. A financial institution cannot disclose to any person, other than to FinCEN, the institution's primary regulator, or the law enforcement agency on whose behalf FinCEN is requesting information, the fact that FinCEN has requested or obtained information.

Financial institutions should retain documentation of all required searches that were performed. If the financial institution elects to maintain copies of the section 314(a) requests, it should not be criticized for doing so, as long as it appropriately secures them and protects their confidentiality. Audits should include an evaluation of compliance with these guidelines within their scope.

Financial institutions should develop and implement comprehensive policies, procedures, and processes for responding to section 314(a) requests. The regulation restricts the use of the information provided in a section 314(a) request (31 CFR 1010.520(b)(3)(iv)). A financial institution may only use the information to report the required information to FinCEN, to determine whether to establish or maintain an account or engage in a transaction, or to assist in BSA/AML compliance.

While the section 314(a) subject list could be used to determine whether to establish or maintain an account, FinCEN discourages financial institutions from using this as the sole factor in reaching a decision to do so unless the request specifically states otherwise. Unlike the OFAC lists, section 314(a) subject lists are not permanent "watch lists" and 314(a) subject lists generally relate to one-time inquiries and are not updated or corrected if an investigation is dropped, a prosecution is declined, or a subject is exonerated. Further, the names do not correspond to convicted or indicted persons; rather a 314(a) subject need only be "reasonably suspected" based on credible evidence of engaging in terrorist acts or money laundering. Moreover, FinCEN advises that inclusion on a section 314(a) subject list should not be the sole factor used to determine whether to file a SAR[47].

Actions taken pursuant to information provided in a request from FinCEN do not affect a financial institution's obligations to comply with all of the rules and regulations of OFAC nor do they affect a financial institution's obligations to respond to any legal process. Additionally, actions taken in response to a request do not relieve a financial institution of

[47] Taken from FFIEC BSA/AML Examination Manual: Information Sharing (accessed 9/13/19)

its obligation to file a SAR and immediately notify law enforcement, if necessary, in accordance with applicable laws and regulations.

Voluntary Information Sharing – Section 314(b) of the USA PATRIOT Act

Section 314(b) (31 CFR 1010.540) encourages financial institutions to share information in order to identify and report activities that may involve terrorist activity or money laundering. Section 314(b) also provides specific protection from civil liability[48]. To avail itself of this statutory safe harbor from liability, a financial institution must notify FinCEN of its intent to engage in information sharing and that it has established and will maintain adequate procedures to protect the security and confidentiality of the information. Failure to comply with the requirements of 31 CFR 1010.540 will result in loss of safe harbor protection for information sharing and may result in a violation of privacy laws or other laws and regulations.

If a financial institution chooses to voluntarily participate in section 314(b), policies, procedures, and processes should be developed and implemented for sharing and receiving of information. The financial institution should designate a point of contact for receiving and providing information. A financial institution should establish a process for sending and receiving information sharing requests. Additionally, a financial institution must take reasonable steps to verify that the other financial institution with which it intends to share information has also submitted the required notice to FinCEN. FinCEN provides participating financial institutions with access to a list of other participating financial institutions and their related contact information.

If a financial institution receives such information from another financial institution, it must also limit use of the information and maintain its security and confidentiality (31 CFR 1010.540(b)(4)). Such information may be used only to identify and, where appropriate, report on money laundering and terrorist activities; to determine whether to establish or maintain an account; to engage in a transaction; or to assist in BSA compliance.

It is important to note that section 314(b) does not authorize a financial institution to share a SAR or to disclose the existence or nonexistence of a SAR. If a financial institution shares information under section 314(b) about the subject of a prepared or filed SAR, the information shared should be limited to underlying transaction and customer information. A financial institution may use information obtained under section 314(b) to determine whether to file a SAR, but the intention to prepare or file a SAR cannot be shared with another financial institution.

Additionally, any actions taken pursuant to information obtained through the voluntary information sharing process do not affect a financial institution's obligations to respond to any legal process. Additionally, actions taken in response to information obtained through the voluntary information sharing process do not relieve a financial institution of its

[48] See FinCEN *Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act* (issued 6/16/09)

obligation to file a SAR and to immediately notify law enforcement, if necessary, in accordance with all applicable laws and regulations.

It is important to note that participation in the section 314(b) information sharing program is *voluntary* and not all RMLOs participate. According a FinCEN report, only 34 mortgage companies participated in section 314(b) information sharing in 2016. By comparison, 6,210 depository institutions participated in section 314(b) that same year[49].

FinCEN provides financial institutions with detailed guidance and instructions relating to sections 314(a) and 314(b). Examiners should review this guidance when examining a RMLO for compliance with sections 314(a) and (b) of the USA PATRIOT Act (if part of the exam scope): FinCEN USA PATRIOT Act Resource.

The Examination Procedures specific to sections 314(a) and 314(b) are located under the **BSA/AML Program Exam Procedures** and start on page 64.

Federal Safe Harbor and Limitation on Liability

31 U.S.C. 5318(g)(3) provides protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to the SAR instructions. The safe harbor applies to SARs filed within the required reporting thresholds as well as to SARs filed voluntarily on any activity below the threshold.

Specifically, the law provides that a RMLO and its directors, officers, employees, and agents that make a disclosure to the appropriate authorities of any possible violation of law or regulation, including a disclosure in connection with the preparation of SARs.

> *"shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure."*

Additionally, a RMLO and any director, officer, employee, or agent that makes a voluntary disclosure of any possible violation of law or regulation to a government agency or makes a disclosure pursuant to 31 CFR §1029.320 or any other authority, including a disclosure made jointly with another institution, shall be protected from liability for any such disclosure, or for failure to provide notice of such disclosure to any person identified in the disclosure, or both, to the full extent provided by 31 U.S.C. 5318(g)(3).

[49] FinCEN *314(b) References in Suspicious Activity Reports (SARs) Suggest Increased Information Sharing Among Financial Institutions* (issued 9/17)

Maintaining the Confidentiality of Suspicious Activity Reports

FinCEN requires all financial institutions and regulatory and law enforcement agencies to preserve the confidentiality of SAR filings. The unauthorized disclosure of SARs could undermine ongoing and future investigations by tipping off suspects, deter financial institutions from filing SARs, and threaten the safety and security of institutions and individuals who file SARs. Additionally, the disclosure of SARs compromises the essential role SARs play in protecting our financial system and in preventing and detecting financial crimes and terrorist financing[50].

FinCEN encourages organizations and authorities, both governmental and non-governmental, to be vigilant in ensuring SAR confidentiality is maintained. This includes making certain all individuals appropriately entrusted with information in a SAR are informed of their obligation to maintain SAR confidentiality. This obligation also applies to any information that would reveal the existence of the SAR[51]. Individuals should also be informed of the consequences for failing to maintain such confidentiality.

The unauthorized disclosure of SARs is a violation of federal law and both civil and criminal penalties may be imposed for SAR disclosure violations. Violations may be enforced through civil penalties of up to $100,000 for each violation and criminal penalties of up to $250,000 and/or imprisonment not to exceed five years. In addition, financial institutions could be liable for civil money penalties resulting from BSA/AML Program deficiencies (i.e. internal controls, training, etc.) that led to the improper SAR disclosure. Such penalties could be up to $25,000 per day for each day the violation continues[52].

The obligation to preserve the confidentiality of SARs applies equally to government officials and SARs must remain confidential even if law enforcement or regulatory authorities obtain them directly from financial institutions. Regulatory authorities should implement programs to protect the confidentiality of SARs and information that would reveal the existence of a SAR.

Examination Procedures

Pre-Examination Scoping and Planning

The 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. As a first step, state examiners should request and review the 23 information request items that are outlined below and included in the **MMC Origination** and **Servicing Information Request templates**.

---

[50] FinCEN Guidance: *Maintaining the Confidentiality of Suspicious Activity Reports* (issued 11/23/10)
[51] See 31 U.S.C. § 5318(g)(2). SAR confidentiality provisions clarify that both the SAR and any information that would reveal the existence of a SAR is confidential and shall not be disclosed except as specifically authorized.
[52] 31 U.S.C. §5321(a)(1)

After receiving the information request items from a RMLO and prior to completing the **BSA/AML Program Exam Procedures**, state examiners should review the two most recent BSA/AML Program risk assessments and independent tests/audits to identify the specific BSA/AML risks applicable to the RMLO and to determine which Examination Procedures to review and/or target. These documents will also assist state examiners in evaluating the overall adequacy and effectiveness of a specific BSA/AML Program.

BSA/AML Program Information Request Items:

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.*

BSA/AML Program Exam Procedures

BSA/AML Examination Procedures	Y	N	Examiner Notes *Document supporting evidence and note determinations and findings made*
BSA/AML Risk Assessment			
1. Determine whether the process for periodically reviewing and updating its BSA/AML risk assessment is adequate.			
2. Determine whether the risk assessment incorporates any third-party vendors and other RMLOs.			
3. Determine whether the RMLO has included all risk areas, including • products, • services, • evolving technologies • mortgage fraud • targeted customers • geography (see HIDTA and HIFCA considerations) • Form 8300s filed • SARs filed • OFAC matches • 314(a) and 314 (b) information sharing programs			
4. The risk assessment should identify and list detailed characteristics for business activities, including, but not limited to: • Origination Channels • Broker Activities • Broker Relationships • Correspondent Relationships • Servicing Activities • Loans originated by the RMLO and/or agents, • Loans purchased from other RMLOs, or • Loans serviced, but not owned by the RMLO			
5. Discuss the RMLO's BSA/AML risk profile and any identified deficiencies in the BSA/AML risk assessment process with senior management.			
BSA/AML Program			
6. Review the board or senior management approved written BSA/AML Program to ensure it contains the following required elements:			

a) A system of internal policies, procedures, and controls to ensure ongoing compliance. b) A designated person or persons responsible for managing BSA compliance (compliance officer). c) Training for appropriate personnel. d) Independent testing of BSA compliance			
7. Based on the documentation provided in the information requests, determine whether the BSA/AML Program appropriate for the size, complexity and risk profile of the RMLO.			
8. Determine whether the BSA/AML Program includes the Customer Identification Program (CIP) or whether it is a standalone program (see **Customer Identification Program (CIP) Exam Procedures**).			
9. Assess whether the board and/or senior management receives adequate reports on BSA/AML compliance.			
10. Determine whether the BSA/AML compliance program includes policies, procedures, and processes that: • Appropriately tailored to the RMLO's risk profile; • Identify higher-risk operations; • Provide for periodic updates to the risk profile; • Inform the board of directors, or a committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies, SARs filed, and corrective action taken. • Identify a person or persons responsible for BSA/AML compliance. • Provide for program continuity despite changes in management or employee composition or structure. • Meet all regulatory requirements, meet recommendations for BSA/AML compliance, and provide for timely updates to implement changes in regulations.			

• Implement risk-based CIP, OFAC policies, procedures, and processes specific to customer identification requirements. • Identify reportable transactions and accurately file all required reports, including SARs, • Provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity. • Provide for adequate supervision of employees that complete reports, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations. • Train employees to be aware of their responsibilities under the BSA regulations and internal policy guidelines. • Record retention requirement (verify that all records are maintained for at least 5 years) • Incorporate BSA compliance into job descriptions and performance evaluations of appropriate personnel.			
BSA Compliance Officer			
11. Determine whether the board of directors has designated a person or persons responsible for the overall BSA/AML compliance program.			
12. Determine whether the BSA compliance officer has the necessary authority and resources to effectively execute all duties under the BSA/AML Program			
13. In reviewing the information request, including resumes and qualifications, assess the competency and level of authority of the BSA compliance officer and any staff.			
14. Assess lines of communication between the compliance officer and personnel and determine effectiveness of the communications.			
15. Determine whether the BSA compliance area is sufficiently staffed for the overall risk level, size, and BSA/AML compliance needs.			

16. Ensure that no conflict of interest exists, and that staff is given adequate time to execute all BSA/AML duties.			
17. Review reports presented to the board or senior management on BSA/AML compliance.			
Training			
18. Determine whether the following elements are adequately addressed in the training materials: • Employee accountability for ensuring BSA compliance. • Specific risks of individual business lines. • BSA/AML policies, procedures, processes. • New rules and regulations. • Red flags and suspicious activity as they relate to the RMLO. • Penalties for noncompliance with internal policies and regulatory requirements.			
19. Determine whether the training program: • Appropriately documents attendance of training courses. • Contains business line specific training. • Has board and upper management buy-in.			
20. Review how staff competency is measured (testing, test score) and if targeted training is provided.			
21. Review training program and records of new staff to ensure overview of BSA/AML requirements given during employee orientation.			
22. Review documentation of training provided to the board and senior management, including attendance records.			
23. Utilize discussions with RMLO managers as needed to gather information and discuss procedures and practices followed by personnel to ensure compliance with laws and regulations.			
24. Review periodic training of BSA compliance officer to ensure it is relevant and appropriate to RMLO risk profile.			
Independent Testing			

25. Determine whether the BSA/AML testing (audit) is independent (i.e. not performed by anyone on the BSA/AML compliance staff) and whether persons conducting the testing report directly to the board of directors or senior management.			
26. Evaluate the qualifications of the independent parties performing the independent testing to assess whether the RMLO can rely upon the findings and conclusions.			
27. Validate the auditor's reports and workpapers to determine whether the independent testing is comprehensive, accurate, adequate, and timely. The independent test should address the following: • The overall adequacy and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes. Typically, this evaluation will include an explicit statement about the BSA/AML compliance program's overall adequacy and effectiveness and compliance with applicable regulatory requirements. At the very least, the audit should contain sufficient information for the reviewer (an examiner, review auditor, or BSA officer) to reach a conclusion about the overall quality of the BSA/AML compliance program. • BSA/AML risk assessment. • BSA reporting and recordkeeping requirements. • CIP implementation. • Personnel adherence to the BSA/AML policies, procedures, and processes. • Appropriate monitoring and testing, with particular emphasis on higher-risk operations. • Training, including its comprehensiveness, accuracy of materials, the training schedule, and attendance tracking.			

• The integrity and accuracy of any monitoring systems. • Tracking of previously identified issues and deficiencies and verification that they have been corrected by management. • If an automated monitoring system is not used to identify or suspicious activity, review processes or controls specific to manual reviews and determine their effective in identifying suspicious activity, including whether the processes and controls are department and responsibility specific.			
28. Determine whether the audit's review of suspicious activity monitoring includes an evaluation of the ability to identify suspicious activity. Ensure that the independent testing: • Reviews policies, procedures, and processes for suspicious activity monitoring. • Evaluates the methodology for establishing and applying expected activity or filtering criteria. • Determines whether the filtering criteria is reasonable and includes, at a minimum higher-risk products, services, customers, or geographies, as appropriate.			
29. Determine whether the audit's review of suspicious activity escalation process includes an evaluation of the research and referral of suspicious activity. Ensure that the independent testing includes a review of policies, procedures, and processes for referring unusual activity from all business lines (i.e. sales/loan origination, processing, underwriting, closing, etc.) to the personnel or department responsible for evaluating suspicious activity.			
30. Review the audit scope, procedures, and workpapers to determine adequacy of the audit based on the following: • Overall audit coverage and frequency in relation to the risk profile of the RMLO.			

• Board reporting and supervision of, and its responsiveness to, audit findings. • Adequacy of its suspicious activity monitoring. • Competency of the auditors or independent reviewers regarding BSA/AML requirements.			
Fraud Prevention			
31. Review the BSA/AML Program to determine if policies, procedures, or processes exist for the risk management and detection of red flags and fraud.			
32. Review the preceding report of examination and fraud-related exceptions noted and determine whether management has taken appropriate corrective action.			
33. Review the results of the various examination programs to determine if problems exist that may be symptomatic of fraud. In cases where fraud may be likely, investigate such problems to determine the cause of the problem (i.e. poor staff training, oversight).			
Suspicious Activity Reporting			
34. Review the policies, procedures, and processes for identifying, researching, and reporting suspicious activity and determine whether they include the following: • Department-specific procedures that detail how the department identifies and escalates suspicious activity to BSA/AML personnel. • Lines of communication for the referral of unusual activity to appropriate personnel. • Designation of individual(s) responsible for identifying, researching, and reporting suspicious activities. • Monitoring systems used to identify unusual activity. • Procedures for reviewing and evaluating the transaction activity of subjects included in law enforcement requests (e.g., grand			

jury subpoenas, section 314(a) requests, etc.). • Evaluating the account of the target for suspicious activity. • Filing SARs, if necessary. • Handling account closures (i.e. mortgage denials).			
35. Review the RMLO's monitoring systems and how the system(s) fits into the overall suspicious activity monitoring and reporting process. When evaluating the effectiveness of the monitoring systems, examiners should consider the RMLO's overall risk profile (higher-risk products, services, customers, and geographic locations), volume of transactions, and adequacy of staffing.			
36. Determine whether any monitoring systems (manual or automated) use reasonable filtering criteria to identify suspicious activity.			
37. Determine whether the RMLO has policies, procedures, and processes to ensure the timely review of and response to potentially suspicious activity reported by staff.			
38. Determine whether policies, procedures, and processes require appropriate research when a suspicious activity is identified.			
39. Evaluate the policies, procedures, and processes for referring suspicious activity from all business lines to the personnel or department responsible for evaluating suspicion activity.			
40. Verify that BSA/AML staffing levels are sufficient to handle alerts and evaluate the activity; and that staff possess the requisite experience level and proper investigatory tools. The policies, procedures, and processes should not be tailored to meet existing BSA/AML staffing levels.			
41. Determine whether the SAR decision process appropriately considers all available customer information under OFAC and CIP.			
42. Determine whether the policies, procedures, and processes provide for:			

• Documenting decisions not to file a SAR. • Escalating issues identified as the result of repeat SAR filings. • Considering closing accounts as a result of continuous suspicious activity.			
43. Determine whether the policies, procedures, and processes provide for: • Completing, filing, and retaining SARs and their supporting documentation. • Reporting SARs to the board of directors, or a committee thereof, and informing senior management.			
44. On the basis of a risk assessment, prior examination reports, any audit findings, and specific documentation provided in the information request, sample specific loan files to review the following: • Suspicious activity identified. • Escalation process. • Timing from initial identification of suspicious activity to reporting to appropriate personnel. • Evaluation of the suspicious activity. • SAR filing is a SAR was filed. • Decisions not to file a SAR. • SAR was filed within 30 calendar days after the initial detection or 60 days according with regulation. • Verify if continuing SARs were required and if so if the SAR was filed timely.			
45. Determine whether decisions to file or not file a SAR are supported and reasonable, whether documentation is adequate, and whether the decision process is completed, and SARs are filed in a timely manner.			
46. Review the quality of SAR content to assess the following: • SARs contain accurate information. • SAR narratives are complete and thorough, and clearly explain why the activity is suspicious.			

47. Based on the assessment of documents in items 44-46 above, determine whether the RMLO failed to identify any reportable suspicious activity.			
48. Determine whether the suspicious activity monitoring systems effectively detect unusual or suspicious activity. Identify the underlying cause of any deficiencies in the monitoring systems (i.e. inappropriate filters, insufficient risk assessment, or inadequate decision-making).			
49. Does the RMLO's BSA/AML Program include risk-based measures to ensure the confidentiality of SARs? ***50.*** *This could include appropriate security measures, limited or restricted access to SAR data, etc.*			
51. On the basis of examination procedures completed, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with monitoring, detecting, and reporting suspicious activity.			
Form 8300 Filings (cash in excess of $10,000)			
52. Review BSA/AML Program to verify that it addresses Form 8300 reporting requirements and includes any policies, procedures, or processes.			
53. Select a sample from accounting records to determine cash handling transactions that are required to be filed on Form 8300. Specifically, verify appropriate documents and accounting records to determine if the RMLO has received cash in excess of $10,000 in any transaction or consecutive or related reportable transactions. If yes, determine whether Form 8300 was filed on such transaction(s).			
54. The RMLO should be alerted to red flags and the need to identify transactions that may indicate attempts to avoid reporting requirements, such as: • A single transaction structured as multiple transactions of less than $10,000; • Transactions in excess of $10,000 where cash and non-cash			

payments appears to be combined to avoid the filing requirements; • A pattern or series of transactions of less than $10,000 conducted over a relatively short period of time by or for the same person. Verify whether procedures specific to Form 8300 address these red flags.			
Foreign Bank and Financial Accounts Reporting (FBAR)			
55. Determine whether the RMLO has a financial interest in, or signature authority over, bank, securities, or other financial accounts in a foreign country, or whether is otherwise required to file a Report of Foreign Bank and Financial Accounts (FBAR). If applicable, review the RMLO's policies, procedures, and processes for filing annual reports.			
56. If applicable, on the basis of a risk assessment, prior examination reports, and a review of any examination findings, select a sample of accounts to determine whether the company has appropriately completed, submitted, and retained copies of the FBAR forms.			
57. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with FBARs.			
Information Sharing with Law Enforcement – Section 314(a)			
58. Verify that the RMLO has sufficient policies, procedures, and processes to document compliance; maintain sufficient internal controls; provide ongoing training; and independently test its compliance with 31 CFR 1010.520, which implements section 314(a) of the USA PATRIOT Act. At a minimum, the procedures should accomplish the following: • Designate a point of contact for receiving information requests. • Ensure that the confidentiality of requested information is safeguarded.			

• Establish a process for responding to FinCEN's requests. • Establish a process for determining if and when a SAR should be filed.			
59. If applicable, determine whether the search policies, procedures, and processes the financial institution uses to respond to section 314(a) requests are comprehensive and cover all records identified in the General Instructions for such requests, including searching accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last six months.			
60. If applicable, if the RMLO uses a third-party vendor to perform or facilitate searches, determine whether an agreement or procedures are in place to ensure confidentiality.			
61. If applicable, review internal controls and determine whether the RMLO's documentation to evidence compliance with section 314(a) requests is adequate.			
Voluntary Information Sharing – Section 314(b)			
62. Determine if the RMLO participates in the voluntary information sharing program under Section 314(b). If yes, complete items 63-67 below.			
63. Verify that the RMLO notified FinCEN of its intent to engage in information sharing and provides an effective date for the sharing of information that is within the previous 12 months.			
64. Verify that the RMLO has policies, procedures, and processes to document compliance; maintain adequate internal controls; provide ongoing training; and independently test its compliance with 31 CFR 1010.540 which implements section 314(b) of the USA PATRIOT Act. At a minimum, the procedures should: • Designate a point of contact for receiving and providing information. • Ensure the safeguarding and confidentiality of information received and information requested.			

• Establish a process for sending and responding to requests, including ensuring that other parties with whom the financial institution intends to share information (including affiliates) have filed the proper notice. • Establish procedures for determining whether and when a SAR should be filed.			
65. If the RMLO is sharing information with other entities and is not following the procedures outlined in 31 CFR 1010.540(b), notify the examiners reviewing the privacy rules.			
66. Through a review documentation on a sample of the information shared and received, evaluate how the RMLO determined whether a SAR was warranted. The RMLO is not required to file SARs solely on the basis of information obtained through the voluntary information sharing process.			
67. On the basis of examination procedures completed, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with information sharing.			

*These examination procedures were taken from the FFIEC BSA/AML Core Examination Procedures specific to BSA/AML, Suspicious Activity Reporting, BSA/AML Compliance Program Structures, and Information Sharing. The examination procedures were condensed to list the examination procedures applicable to RMLOs. The complete BSA/AML Examination Procedures can be accessed here. If needed, Appendix R provides detailed Enforcement Guidance.

Office of Foreign Assets Control (OFAC) Exam Procedures

While OFAC regulations are not part of the Bank Secrecy Act (BSA), evaluation of OFAC compliance is frequently included in BSA/AML Program examinations. The primary role of agencies is not to identify OFAC violations, but rather to evaluate the sufficiency and implementation of policies, procedures, and controls to ensure compliance with OFAC[53].

OFAC Examination Procedures	**Y**	**N**	**Examiner Notes** *Document supporting evidence and note determinations and findings made*
1. Determine whether RMLO has developed policies, procedures, and processes to			

[53] See FFIEC BSA/AML Examination Procedures: Scoping and Planning (accessed 9/17/19)

ensure compliance with OFAC laws and regulations.			
2. To facilitate an understanding of the RMLO's risk profile and to adequately establish the scope of the OFAC exam: • Review the OFAC risk assessment (may be incorporated into the BSA/AML risk assessment) to determine that it consider the various types of products, services, customers, entities, transactions, and geographic locations in which the RMLO • Review the independent testing of its OFAC compliance program. • If applicable, review any correspondence between the RMLO and OFAC.			
3. Review the RMLO's OFAC Compliance Program considering the following: • The extent of, and method for, conducting OFAC searches of each relevant department or channel as the process may vary from one department or channel to another. • The assignment of responsibilities within the institution for ensuring compliance with OFAC. • Timeliness of obtaining and updating OFAC lists and filtering criteria. • The appropriateness of the filtering criteria used to reasonably identify OFAC matches (e.g., the extent to which the filtering or search criteria includes misspellings and name derivations). • The process used to investigate potential matches, including escalation procedures for potential matches. • The process used to block and reject transactions. • The process used to inform management of blocked or rejected transactions. • The adequacy and timeliness of filing to OFAC. • The record retention requirements (*records must be maintained for five years*).			

4. Determine the adequacy of independent testing (audit) and follow-up procedures.			
5. Review the adequacy of the OFAC training program based on the RMLO's OFAC risk assessment.			
Transaction Testing			
6. Sample loans files and evaluate the filtering process used to search the OFAC database (e.g., the timing of the search), and documentation maintained evidencing the searches.			
7. If a third-party system is used to conduct searches, assess the timing of when updates are made to the system, and when the most recent OFAC changes were made to the system. If there is any doubt regarding the effectiveness of the OFAC filter, then run tests of the system by entering test account names that are the same as or similar to those recently added to the OFAC list to determine whether the system successfully identifies a potential hit.			
8. If a third-party system is not used to conduct searches, evaluate the process used to check the loan applicant(s) against the OFAC list and the frequency of such checks.			
9. Review a sample of potential OFAC matches and evaluate the blocking and rejecting processes.			
10. If applicable, review a sample of blocked and rejected reports filed to OFAC and evaluate their completeness and timeliness.			
11. Pull a sample of false hits (potential matches) to check their handling; the resolution of a false hit should take place outside of the business line.			
12. If any potential matches that were not reported to OFAC are identified, discuss with management and advise them to immediately notify OFAC of unreported transactions. Ensure the mortgage application was denied.			
13. If applicable, determine the origin of deficiencies (e.g., training, audit, risk assessment, internal controls, management oversight), and conclude on the adequacy of the OFAC Compliance Program.			
14. Discuss OFAC related examination findings with management.			
15. Include OFAC conclusions within the report of examination, as appropriate.			

*These examination procedures were taken from the FFIEC BSA/AML Core Examination Procedures specific to OFAC and condensed to include only the items applicable to RMLOs. The complete OFAC Examination Procedures can be accessed here.

Customer Identification Program (CIP) Exam Procedures

Customer Identification Program (CIP) Examination Procedures	**Y**	**N**	**Examiner Notes** *Document supporting evidence and note determinations and findings made*
1. Verify that the RMLO's BSA/AML Program and associated policies, procedures, and processes include a comprehensive program for identifying customers who apply for a loan.			
2. The policies, procedures, and processes at a minimum include: • Procedures for complying with recordkeeping requirements; • Procedures for checking new accounts against prescribed government lists; • Procedures for providing adequate customer notice; • Procedures covering the reliance on another financial institution or a third party, if applicable; • Procedures for determining whether and when a SAR should be filed.			
3. Do the policies, procedures, and processes identify what information is required to be obtained and address situations in which verification cannot be performed?			
4. Does the CIP take into account the types of accounts offered; methods of applying for a loan; and the RMLO's size, location, and customer base?			
5. Review board minutes and verify that the board of directors approved the CIP, either separately or as part of the BSA/AML Program.			
6. Evaluate the BSA/AML audit and training programs to ensure that the CIP is adequately incorporated.			
7. Evaluate the policies, procedures, and processes for verifying that all new accounts are checked against prescribed government lists for suspected terrorists or terrorist organizations on a timely			

basis. Also see *OFAC Examination Procedures*.			
Transaction Testing			
8. On the basis of a risk assessment, prior examination reports, and a review of any audit findings, select a sample of loans opened since the most recent exam to review for compliance with the CIP.			
9. From the sample of loans, determine whether the RMLO has performed the following procedures: • Opened the account in accordance with the requirements of the CIP; • Formed a reasonable belief as to the true identity of a customer, including a higher-risk customer; • Obtained from each customer, before opening the account, the identity information required by the CIP; • Within a reasonable time after account opening, verified enough of the customer's identity information to form a reasonable belief as to their true identity; • Appropriately resolved situations in which customer identity could not be reasonably established; • Maintained a record of the identity information required by the CIP, the method used to verify identity, and verification results (including results of discrepancies); • Compared the customer's name against the list of known or suspected terrorists or terrorist organizations; • Filed SARs, as appropriate.			
10. If applicable, select a sample of relationships with third parties the RMLO relies on to perform its CIP (or portions of its CIP) to determine: • Whether the third party is a federally regulated institution subject to a final rule implementing the AML program requirements of 31 USC 5318(h); • Whether reliance is reasonable. The contract and certification			

should provide a standard means for a RMLO and third party to demonstrate that it has satisfied the "reliance provision".			
11. If the RMLO is using an agent or service provider to perform elements of its CIP, determine whether the RMLO has established appropriate internal controls and review procedures to ensure that its CIP is being implemented for third-party agent or service-provider relationships.			
12. Review sample loan files to determine the adequacy of the customer notice and the timing of the notice's delivery.			
13. Evaluate the CIP record retention policy and ensure that it corresponds to the regulatory requirements. The RMLO must retain the identity information obtained at account opening for five years after the account closes. The RMLO must also maintain a description of documents relied on, methods used to verify identity, and resolution of discrepancies for five years after the record is made.			
14. Include CIP conclusions within the report of examination, as appropriate.			

*These examination procedures were taken from the FFIEC BSA/AML Core Examination Procedures specific to CIP and condensed to include only the items applicable to RMLOs. The complete CIP Examination Procedures can be accessed here.

Identity Theft Prevention Exam Procedures

Identity Theft Prevention Examination Procedures	**Y**	**N**	**Examiner Notes** *Document supporting evidence and note determinations and findings made*
1. Verify the RMLO has a risk-based, written Identity Theft Prevention Program designed to detect the "red flags" of identity theft.			
2. Verify that senior management or the board of directors initially approved the BSA/AML Program, and that there is a qualified, designated committee or individual involved in the implementation and administration of the Program.			
3. The Program is appropriately tailored to the size and complexity of the RMLO and contains reasonable policies and procedures to, at a minimum:			

a) Identify red flags for the accounts the RMLO offers or maintains and incorporate those red flags into the Program; b) Detect red flags that have been incorporated into the Program; c) Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and d) Ensure the Program (including the red flags determined to be relevant) is updated periodically to reflect changes in risks to customers and to the safety and soundness of the RMLO from identity theft.			
4. The Program appropriately considers the following factors in identifying relevant Red Flags that apply to the RMLO: a) The types of covered accounts it offers or maintains; b) The methods it provides to open its covered accounts; c) The methods it provides to access its covered accounts; and d) Its previous experiences with identity theft.			
5. The Program considered and incorporated the appropriate guidelines in Supplement A to Appendix A in the formulation of its Program.			
6. The Program addresses the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by: a) Obtaining identifying information and verifying the identity of a person opening a covered account (also see Customer Identification Program); and b) Authenticating customers and monitoring transactions (if applicable)			
7. Determine whether the Program has effective policies and procedures in place to escalate red flags or situations involving, or may involve, identity theft.			
8. Determine whether the RMLO uses technology to detect red flags.			

• *If yes, discuss with management the methods by which the financial institution confirms the technology is working effectively*.			
9. Review any reports (i.e. audit reports, annual reports for management or an appropriate committee, etc.) on compliance with the Red Flags Rule, to determine if the reports address: • The effectiveness of the Program; • Significant incidents of identity theft and management's response; • Oversight of service providers that perform activities related to covered accounts; and • Recommendations for material changes to the Program (if applicable, determine whether management adequately addressed any deficiencies)			
10. Verify that the RMLO trains appropriate staff to effectively implement and administer the Program.			
11. If the RMLO uses a third party to perform activities under the Program, determine whether the RMLO ensures the third party has procedures in place to detect red flags and either report them to the RMLO or respond appropriately to prevent or mitigate the crime.			
12. Determine whether the Program (including the red flags determined to be relevant) is updated periodically to reflect changes in the risks to customers and the safety and soundness of the RMLO from identity theft.			
13. Are there any findings in other areas (BSA, CIP, OFAC) that may suggest existing deficiencies that adversely affect the RMLO's ability to comply with the Identity Theft Red Flags Rules?			
Fraud and Active Duty Alerts – Section 605A(h); 15 U.S.C. 1681c-1(h) regarding the circumstances in which credit may be extended when the RMLO detects fraud or an active duty alert.			
14. Determine whether the RMLO has effective policies and procedures in place to verify the identity of consumers in situations in which consumer reports			

include fraud and/or active duty military alerts.			
15. Determine if the RMLO has effective policies and procedures in place to contact consumers in situations where consumer reports include extended alerts.			
16. If procedural weaknesses or other risks requiring further investigation are noted, review a sample of transactions in which consumer reports including these types of alerts were obtained. Verify that the entity complied with the identity verification and/or consumer contact requirements.			
Information Available to Victims – Section 609(e); 15 U.S.C. 1681g(e)			
17. Review the RMLO's policies, procedures, and/or practices to determine whether identities and claims of fraudulent transactions are verified and whether information is properly disclosed to victims of identity theft and/or appropriately authorized law enforcement agents.			
18. If procedural weaknesses or other risks requiring further investigation are noted, review a sample of these types of requests to determine whether the entity properly verified the requestor's identity prior to disclosing the information.			

*These examination procedures were taken from the Red Flags Rule and the CFPB FCRA Examination Procedures Module 5: Consumer Alerts and Identity Theft Protections (items 14-18). The FCRA contains several provisions for both consumer reporting agencies and users of consumer reports, including financial institutions, that are designed to help combat identity theft. Two primary requirements exist for *users* of consumer reports:

1. A user of a consumer report that contains a fraud or active duty alert must take steps to verify the identity of an individual to whom the consumer report relates; and
2. A person must disclose certain information when consumers allege that they are the victims of identity theft.