MMC MORTGAGE EXAMINATION MANUAL

Bank Secrecy Act / Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements

MULTI-STATE MORTGAGE COMMITTEE
1129 20th Street, NW, Ninth Floor
Washington, D.C. 20036
Telephone: (202) 728-5756 ● Facsimile (202) 728-0000

Table of Contents

Overview 2
Anti-Money Laundering Program 4
Introduction 4
Internal Controls and Procedures 5
Designation of a Compliance Officer 5
Training 6
Independent Testing 7
Examination Objectives and Procedures 8
Reporting Requirements 14
Suspicious Activity Reports 15
Form 8300 15
Form 8300 Red Flags 17
Foreign Bank and Financial Accounts Reports (FBARs) (31 CFR 1029.300) 18
Report of International Transportation of Currency or Monetary Instruments (CMIRs) (31 CFR 1029.300) 18
Information Sharing Reports 314(a) and 314(b) 18
Information Sharing Between Government Agencies and Financial Institutions 314(a) (31 CFR 1029.520) 19
Voluntary Information Sharing Among Financial Institutions 314(b) (31 CFR 1029.540) 20
Examination Objectives and Procedures 21
Office of Foreign Assets Control (OFAC) 30
Overview & Exam Procedures 30
Definitions & Acronyms 31
Definitions 31
Acronyms 33

FinCEN's rule applying the Bank Secrecy Act and Anti-Money Laundering requirements to the mortgage industry is effective April 16, 2012 with a compliance date of August 13, 2012.

Overview

The Bank Secrecy Act authorizes the Secretary of the Treasury (the "Secretary") to issue regulations for entities and to keep records and file reports that the Secretary determines have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counter intelligence activities, including analysis, to protect against international terrorism.

Overall authority for enforcement and compliance is delegated by the Secretary to the Director of the Financial Crimes Enforcement Network (FinCEN). Federal regulators have been delegated authority to examine certain financial institutions they oversee for compliance with FinCEN's regulations and the Internal Revenue Service ("IRS") has been delegated the authority, under this regulation to examine financial institutions that are not examined by a Federal regulator.

Prior to conducting Bank Secrecy Act ("BSA")/Anti-Money Laundering ("AML") examinations, state agency representatives that regulate and examine RMLOs should review their specific state financial codes for applicable authority to examine for BSA compliance.

The mortgage market is a diverse industry with various parties involved in the loan process. The purpose of this section of the manual is to provide guidance to examiners for carrying out the BSA/AML examination and Suspicious Activity Reporting for Residential Mortgage Loan Originators ("RMLOs"). Additionally, it is to assist examiners in the evaluation for compliance with the anti-money laundering compliance program implementation and operation, as well as the BSA reporting and recordkeeping requirements under Title 31 CFR Parts 1010 and 1029.

A residential mortgage lender is defined in the BSA regulations as a person to whom the debt arising from a residential mortgage loan is initially payable or the obligation is initially assigned at or immediately after the settlement of the loan. The definition does not include an individual who finances the sale of the individual's own dwelling or real property.

A residential mortgage originator is defined in the BSA regulations as a person whom accepts a residential mortgage loan application or offers or negotiates terms of a residential mortgage loan for compensation or gain. A mortgage broker is included

under this definition and would be required to establish a BSA/AML program and file suspicious activity reports ("SARs").

An RMLO is required to implement risk-based programs that take into account the unique risks associated with that particular business's products and services, as well as the business's size, market, and other issues. Thus, each BSA/AML program may vary due to different product offerings, geography, and other risks.

Mortgage fraud is one of the most significant operational risks facing RMLOs in the ordinary course of business. There are two motivations for mortgage fraud: fraud for house and for profit. Mortgage fraud generally involves material misrepresentation or omission of information, such as income, net worth and employment record, with the intent to deceive or mislead lenders or homeowners.[1] Laundering the proceeds of fraud is the next step once a fraud has generated a benefit. Because of the complexity of the schemes, RMLOs should address mortgage fraud risks as well as mitigations in policies, procedures, and internal controls as well as training.[2]

Commonly reported schemes include:

- *Advance Fee Schemes* deceive homeowners who pay for services upfront to modify loans and never receive services.
- *Debt Elimination Schemes* purports to eliminate borrowers' debt for a fee utilizing fraudulent financial documents claiming the debt has been settled.
- *Straw Borrower Schemes* involve consumers that are paid for the use of their name and credit information, hiding the identity of the true owner.

The motivation behind mortgage fraud is money. This type of profit is often committed with the complicity of industry insiders such as mortgage brokers, real estate agents, appraisers, and settlement agents.[3] It is recognized that this fraud could generate large losses per individual transactions, have multiple misrepresentations per loan file, and the participants often are paid for their part.

In addition, there is a large proportion of mortgage fraud done by misrepresentation of the identity of the potential customer in the origination process. The ID Theft Red Flag

---

1 Mortgage Fraud is defined as a material misstatement, misrepresentation, or omissions relied upon by an underwriter or lender to fund, purchase, or insure a loan. Mortgage loan fraud is divided into two categories: fraud for property and fraud for profit. FBI Financial Crimes Section, Financial Institution Fraud Unit, Mortgage Fraud, A Guide for Investigators, 2003. Additional information on Mortgage Fraud can be found at http://www.fincen.gov/news_room/rp/mortgagefraud.html.

2 Additional information on Mortgage Fraud can be found at http://www.fincen.gov/news_room/rp/mortgagefraud.html.

3 FinCEN, Mortgage Loan Fraud: An Industry Assessment based upon Suspicious Activity Report Analysis, November 2006.*Available at* http://www.fincen.gov/news_room/rp/reports/pdf/MortgageLoanFraud.pdf.

Regulation[4] requires the development and implementation of a written identity theft prevention program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The program must be commensurate to the size and complexity of the company and to the nature of its activities.

The regulation lists the four basic elements that must be included in the program and must contain reasonable policies and procedures to:

- Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the program,
- Detect Red Flags that have been incorporated into the program,
- Respond appropriately to any Red Flags to prevent and mitigate ID theft, and
- Ensure that the program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

Anti-Money Laundering Program

Introduction

RMLOs are required to establish BSA/AML programs that include, at a minimum: (1) the development of internal policies, procedures, and controls; (2) the designation of a compliance officer; (3) an ongoing employee training program; and (4) provide for independent testing to determine BSA compliance. The scope and frequency of the testing shall be commensurate with the risks posed by the company's products and services. Such testing may be conducted by a third party or by an officer or employee of the RMLO, so long as the person is not the compliance officer or reports to the compliance officer.

Section 1029.210 requires that all RMLOs establish, develop, and implement a written anti-money laundering program under a risk-based approach that is reasonably designed to prevent the RMLO from being used to facilitate money laundering or the financing of terrorist activities. The program must be approved by senior management, or in some cases, the Board of Directors depending on the corporate structure of the RMLO.

The four pillars of the BSA/AML program are:

- Internal Controls and Procedures

4 Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003, Federal Register, Vol 72. No. 217, Friday, November 9, 2007, Rules and Regulations. pp 63718–63775. See this document to prepare a risk-based compliance program.

- Designation of a Compliance Officer
- Training
- Independent Testing

Internal Controls and Procedures

RMLO policies, procedures, and internal controls should be commensurate with the size and complexity of the company and based upon the risks associated with its products, type of customers, and services provided. Policies, procedures, and internal controls developed and implemented by an RMLO should include agents and brokers obtaining all relevant customer-related information necessary for an effective BSA/AML program, as required by 31 CFR 1029.210.

As such, a best practice for the RMLO is to document the risk based process utilized to create the BSA/AML program. This document should be reviewed on a regular basis in order to update in a timely manner or as specific circumstances warrants, such as the addition of new products and/or services. The risk assessment needs to identify the company's risk categories (i.e. products, services, customers, transactions, geographic locations) and provide a detailed analysis to assess the level of risk within each category.

As a result of this assessment, the BSA/AML program should be prepared with a complete profile of the RMLO's operation. Having these updates or periodic reviews in writing gives management an invaluable tool to amend policies and procedures. At the same time, the risk assessment provides the first step to establish controls to mitigate those identified risks and to evaluate the adequacy of the internal controls established throughout the company.

Designation of a Compliance Officer

An RMLO must designate a Compliance Officer who is responsible for the effective implementation of the BSA/AML program. This BSA/AML program should include the regular monitoring for compliance by the company's agents and brokers. However, senior management still retains ultimate responsibility to ensure that the RMLO is in compliance with the BSA requirements.

A designated compliance officer is responsible for ensuring that:

- The anti-money laundering program is implemented effectively, including monitoring compliance by the company's agents and brokers with their

obligations under the program;
- The anti-money laundering program is updated as necessary; and
- Appropriate persons are educated and trained to implement and monitor for BSA compliance to the company's BSA/AML program and reporting requirements.

The BSA Compliance Officer can delegate BSA/AML duties to other personnel, but is responsible for the overall compliance of the program. This BSA Compliance Officer is required to be fully knowledgeable of all mortgage related regulations. Additionally, the officer should be knowledgeable on new regulations, and receive timely training relevant to BSA/AML duties.

Senior Management is responsible for ensuring that the BSA Compliance Officer has sufficient authority and resources (monetary, physical, and personnel) to administer an effective BSA/AML compliance program based on the company's risk profile.

The designation of a BSA 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.

The line of communication should allow the BSA Compliance Officer to regularly apprise management of ongoing compliance with the BSA and pertinent BSA-related information. This includes reporting SARs filed with FinCEN to senior management or an appropriate board committee so that these individuals can make informed decisions about overall BSA/AML compliance.

Training

The RMLO must ensure that appropriate personnel are trained in BSA/AML for their respective roles in the company. Training should include regulatory requirements and the company's internal BSA/AML policies, procedures, and processes. At a minimum, the RMLO's training program must provide training for all personnel whose duties require knowledge of the BSA/AML and in all products and services identified in the risk assessment. The training should be tailored to the person's specific responsibilities. In addition, an overview of the BSA/AML requirements typically should be given to new staff during employee orientation.

The BSA Compliance Officer should receive periodic training that is relevant and appropriate given changes to regulatory requirements as well as the activities and overall BSA/AML risk profile of the business activity. Training should be conducted in accordance with the companies' policy and procedures manual. A good practice is for the RMLO to conduct training on an annual basis.

Training should be ongoing and incorporate current developments and changes to the BSA and any related regulations. Changes to internal policies, procedures, processes, and monitoring systems should also be covered during training. The training program should reinforce the importance of the BSA/AML compliance program and ensure that all employees understand their role in maintaining an effective program.

Management should be informed of changes and new developments in the BSA, its implementing regulations and directives. If applicable, while the board of directors may not require the same degree of training as RMLO personnel, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed to the RMLO.

Without a general understanding of the BSA, senior management cannot adequately provide BSA/AML oversight, approve BSA/AML policies, procedures, and processes, or provide sufficient BSA/AML resources.

The RMLO should document their training programs. Training and testing materials, the dates of training sessions, and attendance records should be maintained by the company and be available for examiner review.

An RMLO may satisfy this requirement with respect to its employees, agents, and brokers by directly training such persons or verifying that such persons have received training by a competent third party with respect to the products and services offered by the RMLO.

Independent Testing

An independent testing or audit should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties. Such testing may be conducted by a third party or by any officer or employee of the RMLO so long as it is not the person designated as the Compliance Officer or an individual who reports to the Compliance Officer. While there is no specific frequency of audit, it is a good practice to conduct an independent testing that is commensurate with the BSA/AML risk profile of the company, including agents. The independent testing is to determine whether the RMLO is operating within compliance with the BSA/AML requirements and its own policies and procedures.

Those persons responsible for conducting an objective independent evaluation of the written BSA/AML compliance program should perform testing for specific compliance with BSA/AML, and evaluate pertinent management information systems (MIS). 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. The frequency and depth of each activity's audit will vary according to the activity's risk assessment. Risk-based auditing enables auditors to use the company's risk assessment to focus the audit scope on the areas of greatest concern. The testing should assist management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls.

The review should occur as described in the RMLO's BSA/AML program. The review should be documented by the person or persons conducting the review. The scope of the review, procedures performed, transactions tested, and any findings should be documented.

Examination Objectives and Procedures

Determine that internal controls, policies, and procedures have been established, well implemented and provide adequate compliance with BSA/AML regulations and fraud prevention procedures.

Anti-Money Laundering Program Exam Procedures

	Examination Procedures	Y	N	Examiner Notes [Document supporting evidence and note determinations and findings made]
Scope and Planning				
1	Coordinate examination activities with other members of the examination team and the examiner-in-charge (EIC).			
2	Review prior examination workpapers and management's responses and procedures not completed.			
3	Emphasize identifying violations of law and regulation; integrate those findings with the examination; and draw conclusions on management's compliance with laws and regulations.			

Internal Controls – 31 CFR 1029.210(b)(1)				
4	Review and evaluate the adequacy of policies, procedures, and internal controls in compliance with the requirements of 31 CFR §1029.210, which requires the development and implementation of a risk-based anti-money laundering program. This should also include procedures to file suspicious activities reports (SARs). *Note reviews and approvals by Senior Management, the Board of Directors or owner of the company.*			
5	Verify policy for record retention requirement. Test record retention in 5 years.			
Risk Assessment – 31 CFR 1029.210(b)(1)				
6	Review the company's BSA/AML risk assessment to include lenders and originators, as well as third party vendors.			
7	Determine whether the RMLO has included all risk areas, including ○ new products, ○ services, ○ targeted customers ○ US Citizen ○ Non-US Citizen ○ Professional Service Provider ○ Cash intensive business ○ geography/location of property ○ geography/location of customer business			

	○ Form 8300s filed ○ SARs filed ○ OFAC matches ○ 314(a) match.			
8	Review if the state law allows RMLO's to originate mortgage loans on properties located in other states.			
9	Determine whether the company's process for periodically reviewing and updating its BSA/AML risk assessment is adequate.			
10	The risk assessment should list and identify characteristics for: ○ loans originated by the company and/or agents, ○ loans purchased from other companies, or ○ loans serviced, not owned by the company.			
11	Examiners should document and discuss the company's BSA/AML risk profile and any identified deficiencies in the risk assessment process.			
Compliance Officer – 31 CFR 1029.210(b)(2)				
12	Review designation of the Compliance Officer. The package presented to Senior Management/Board needs to include the resume with a list of jobs and position.			
13	Review reports prepared for Senior Management/Board and daily performance.			
14	Assess competency and overview lines of communication with other personnel.			
15	Review if the BSA area is			

	reasonably staffed for the risk profile due to types of loans offered and any other additional services.			
16	Review reports presented to Senior Management/Board.			
Training Program – 31 CFR 1029.210(b)(3)				
17	Request and review the training program; what is included, dates given and attendance.			
18	Review how staff competency is measured (testing, test score) and targeted training as necessary.			
19	Review attendance of Senior Management/Board members and/or owner.			
20	Utilize discussions with RMLO managers as needed to gather information and discuss procedures and practices followed by institution's personnel to ensure compliance with laws and regulations.			
21	Review documentation of training given to Senior Management, members of the Board, and/or owner.			
22	Review coverage of different scenarios of money laundering, fraud in mortgage transactions and examples of suspicious activities.			
23	Examiners should determine if the following elements are addressed in the training program and materials: ○ Training frequency is specified ○ Attendance records and			

	training material are documented ○ Employees are accountable for ensuring BSA compliance ○ Internal policies, procedures, and new rules and regulations are covered ○ Different forms of money laundering and terrorist financing as it relates to identification is covered ○ Examples of suspicious activity is covered. ○ Competency of staff (testing and test scores)			
Independent Testing – 31 CFR 1029.210(b)(4)				
24	Review the independent testing or audit scope, procedures, and work papers to determine adequacy of the test/audit based on the following: ○ Competency of the auditors or independent reviewers regarding BSA/AML requirements ○ Senior Management/Board reporting and supervision of, and its responsiveness to audit findings. ○ The adequacy of policies and procedures and whether they comply with internal requirements to include the overall audit			

	coverage in relation to the risk profile of the company; ○ Personnel adherence to the company's BSA/AML policies, procedures, and processes. ○ Training adequacy, including its comprehensiveness, accuracy of materials, the training schedule, and attendance tracking.			
25	Determine whether the independent test or audit's review of suspicious activity reporting systems includes an evaluation of the research and referral of unusual activity. Ensure through a validation of the independent reviewer's or auditor's reports and workpapers that the company's independent testing includes a review of policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity.			
Fraud Prevention				
26	Review the RMLO' s fraud risk management program. Determine whether it includes written policies that convey expectations for management regarding managing fraud risk.			
27	Review the preceding report of			

	examination and fraud-related exceptions noted and determine whether management has taken appropriate corrective action.			
28	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 (for example, poor staff training, errors).			
29	Review the company' s independent testing or audit reports to determine if specific procedures exist to detect fraud.			
30	Review and note findings and conclusions, and appropriate recommendations for any necessary corrective measures, on the appropriate work papers and report pages.			

Reporting Requirements

FinCEN's new rule requires RMLOs to file Suspicious Activity Reports, Form 8300 for large cash transactions, Information Sharing Reports 314(a) and 314(b), Foreign Bank and Financial Accounts Reports (FBARs) and Reports of International Transportation of Currency or Monetary Instruments (CMIRs). The following sections provide information on transactions that require a report, when and where to file, and additional information specific to each report. The information below is a summary, and further information and exceptions can be found in the regulation.

Effective July 1, 2012[5] institutions must submit SARs electronically unless they are granted a temporary exemption. Currency and Monetary Instrument Reports (CMIRs) and Form 8300s (Report of Cash Payments over $10,000 Received in a Trade or

5 Additional information on the e-filing mandate is available at http://www.fincen.gov/news_room/nr/pdf/20120629.pdf.

Business) are not subject to mandatory electronic filing at this time. FinCEN also encourages individuals to e-file FBARs (Reports of Foreign Bank and Financial Reports); however the mandatory e-filing deadline has been postponed to June 30, 2013.

Suspicious Activity Reports

Suspicious Activity Reports (SARs) (31 CFR 1029.320) should be made for a transaction that involves or aggregates funds or other assets of at least $5,000, and the RMLO knows, suspects or has reason to be suspect that the transaction (or a pattern of transactions of which the transaction is a part of involves funds derived from illegal activity or is intended or conducted in order to hide or evade any Federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation). This includes structuring or other means to evade any BSA requirement.

Transactions that are deemed to be suspicious have no business or apparent lawful purpose, or are not the sort in which the particular customer would normally be expected to engage, and the RMLOs knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction. Suspicious transactions may also involve the use of the RMLO to facilitate criminal activity.

A Suspicious Activity Report and supporting documentation should be filed with FinCEN in accordance with instructions listed on the SAR no later than 30 days from the date of initial detection of the suspicious transaction. If no suspect is identified on the date of initial detection, the RMLO may delay filing a SAR, but that delay should not extend past 60 days. If a situation occurs that needs immediate attention (terrorist financing or ongoing money laundering schemes), the RMLO should immediately telephone law enforcement authorities in addition to filing a SAR.

An RMLO shall maintain a copy of any SAR filed and the original supporting documentation for a period of 5 years from the date of filing the SAR.

Form 8300

Currency in excess of $10,000 received in one transaction (or two or more related transactions) requires an IRS Form 8300.[6] A copy of each form filed must be kept for five years from the filing date.

Any person who in the course of a trade or business acts as an agent (or in some other similar capacity) and receives currency in excess of $10,000 from a principal must also file an IRS Form 8300.

An exception exists for an agent who receives currency from a principal and uses all of the currency within 15 days in a currency transaction and who discloses the name, address, and TIN of the principal to the recipient in the second currency transaction.

A form 8300 must be filed for the receipt of multiple currency deposits or currency installment payments relating to a single transaction if the initial payment exceeds $10,000.

There are certain exceptions to filing a Form 8300, including the receipt of cashier checks, bank drafts, traveler's checks or money orders received as the proceed of a loan, as a payment on a promissory note, an installment sales contract, or received as a down payment and the payment of the balance of the purchase price by a date no later than the date of the sale. There is no requirement to report a currency transaction if the entire transaction occurs outside the United States (the fifty states and the District of Columbia). If, however, any part of an entire transaction occurs in the Commonwealth of Puerto Rico or a possession or territory of the United States and the recipient of currency in that transaction is subject to the general jurisdiction of the Internal Revenue Service under title 26 of the United States Code, the recipient is required to report the transaction under this section.

The reports required by this section must be filed with the Internal Revenue Service by the 15th day after the date the reportable transaction is received.

A person required to file a report under this section must keep a copy of each return filed for five years from the date of filing.

Additionally, a written or electronic statement must be provided to any person named on a required Form 8300 filed with the Internal Revenue Service. It must contain the following information:

---

6 Currency is defined at 31 CFR 1010.330, *available at* http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=7511cbde3306ffbcef6e6ff4c72f8b86&rgn=div8&view=text&node=31:3.1.6.1.2.3.3.12&idno=31

a. The name and address of the person making the return;
b. The aggregate amount of the reportable transaction received by the person who made the information return required by this section during the calendar year in all cash transactions relating to the identified person; and
c. A legend stating that the information contained in the statement is being reported to the Internal Revenue Service.

Statements must be furnished to an identified person on or before January 31 of the year following the calendar year in which the reportable transaction is received. A statement shall be considered to be furnished to an identified person if it is mailed to the identified person at the identified person's last known address.

Form 8300 Red Flags

The business and/or the customer can potentially be involved in money laundering schemes. The examiner must focus on both the business and the transactor(s) during the Form 8300 compliance review.

Money laundering techniques which could be used by the business include:

- Failing to maintain complete records;
- Failing to maintain accurate records;
- Failing to record specific transactions;
- Failing to file Form 8300 on reportable transactions; and
- Structuring a transaction by breaking one transaction into several to circumvent the reporting requirements.

Money laundering techniques which could be used by the customer/transactor include:

- Using multiple locations to conduct transactions;
- Using several individuals at one or more locations to conduct a transaction;
- Using aliases when conducting transactions;
- Conducting numerous transactions at the same location at different times during one day; and
- Using a combination of currency and monetary instruments to conduct transactions.

Evidence that uncovers potential money laundering schemes should be referred to the appropriate law enforcement agency.

Foreign Bank and Financial Accounts Reports (FBARs) (31 CFR 1029.300)

Any RMLO subject to U.S. jurisdiction with a financial interest in, or signature or other authority over, a bank, a securities, or any other financial account in a foreign country must file a Report of Foreign Bank and Financial Accounts (FBAR) (TD F 90-22.1) with the IRS if the aggregate value of these financial accounts exceeds $10,000 at any time during the calendar year. The term financial account includes accounts in which assets are held in a commingled fund and the account owner holds an equity interest in the fund, as well as debit card and prepaid card account.

An FBAR must be filed with the Commissioner of the IRS on or before June 30 of each calendar year for foreign financial accounts where the aggregate value exceeded $10,000 at any time during the previous calendar year.

Report of International Transportation of Currency or Monetary Instruments (CMIRs) (31 CFR 1029.300)

Each person who physically transports, mails, or ships currency or monetary instrument in excess of $10,000 at one time out of or into the United States must file a CMIR (FinCEN form 105). A CMIR must be filed with the appropriate Bureau of Customers and Border Protection officer or with the commissioner of Customs at the time of entry into or departure from the United States within 15 days of receipt of the instruments. The report is to be completed by or on behalf of the person requesting the transfer of the currency or monetary instruments.

RMLOs are not required to file CMIRs if mailed or shipped through the postal service or by common carrier.

If the customer's activity is unusual and not customary for the type of business a SAR should be filed.

Information Sharing Reports 314(a) and 314(b)

Section 314(a) of the USA PATRIOT Act allows for the sharing of information with federal, state, local and foreign regulatory agencies through established procedures. Section 314(b) establishes parameters for sharing information with other financial

institutions to deter money laundering and terrorist activity. For this section an RMLO is defined as a "financial institution" pursuant to 31 U.S.C. 5312(a)(2).[7]

Information Sharing Between Government Agencies and Financial Institutions 314(a) (31 CFR 1029.520)

A law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on the investigating agency's behalf, certain information from a financial institution or a group of financial institutions. Upon receiving an information request from FinCEN, a financial institution shall expeditiously search its records to determine whether it maintains or has maintained any account for, or has engaged in any transaction with, each individual, entity, or organization named in FinCEN's request.

Except as otherwise provided in the information request, a financial institution shall only be required to search its records for:

- Any current account maintained for a named suspect;
- Any account maintained for a named suspect during the preceding twelve months; and
- Any transaction conducted by or on behalf of a named suspect, or any transmittal of funds conducted in which a named suspect was either the transmittor or the recipient, during the preceding six months that is required under law or regulation to be recorded by the financial institution or is recorded and maintained electronically by the institution.

If a financial institution identifies an account or transaction identified with any individual, entity, or organization named in a request from FinCEN, it shall report to FinCEN, in the manner and in the time frame specified in FinCEN's request, the following information:

- The name of such individual, entity, or organization;
- The number of each such account, or in the case of a transaction, the date and type of each such transaction; and
- Any Social Security number, taxpayer identification number, passport number, date of birth, address, or other similar identifying information provided by the individual, entity, or organization when each such account was opened or each such transaction was conducted.

7 The definition of financial institution under 31 U.S.C. 5312(a)(2) is located at http://www.gpo.gov/fdsys/pkg/USCODE-2011-title31/pdf/USCODE-2011-title31-subtitleIV-chap53-subchapII-sec5312.pdf.

Upon receiving an information request under 314(a), a financial institution shall designate one person to be the point of contact at the institution regarding the request and to receive similar requests for information from FinCEN in the future.

A financial institution can not use information provided by FinCEN pursuant to 314(a) for any purpose other than: Reporting to FinCEN as provided in this section; determining whether to establish or maintain an account, or to engage in a transaction; or assisting the financial institution in complying with any requirement of this chapter.

Nothing in 314(a) can be construed to require a financial institution to take any action, or to decline to take any action, with respect to a relationship established for, or a transaction engaged in with, an individual, entity, or organization named in a request from FinCEN, or to decline to establish a relationship for, or to engage in a transaction with, any such individual, entity, or organization. Except as otherwise provided in an information request under 314(a), such a request cannot require a financial institution to report on future account opening activity or transactions or to treat a suspect list received under 314(a) as a government list.

Voluntary Information Sharing Among Financial Institutions 314(b) (31 CFR 1029.540)

A financial institution or an association of financial institutions may, under the protection of the safe harbor from liability, transmit, receive, or otherwise share information with any other financial institution or association of financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that the financial institution or association suspects may involve possible terrorist activity or money laundering.

A financial institution or association of financial institutions that intends to share information must submit to FinCEN a notice described on FinCEN's Internet Web site, http://www.fincen.gov. Each notice shall be effective for the one year period beginning on the date of the notice. In order to continue to engage in the sharing of information after the end of the one year period, a financial institution or association of financial institutions must submit a new notice.

Prior to sharing information, a financial institution or an association of financial institutions must take reasonable steps to verify that the other financial institution or association of financial institutions with which it intends to share information has submitted to FinCEN the required notice. A financial institution or an association of financial institution may satisfy this by confirming that the other financial institution or association of financial institutions appears on a list that FinCEN will periodically make available to financial institutions or associations of financial institutions that have filed a

notice with it, or by confirming directly with the other financial institution or association of financial institutions that the requisite notice has been filed.

Information received by an financial institution or an association of financial institutions pursuant to this section shall not be used for any purpose other than: Identifying and, where appropriate, reporting on money laundering or terrorist activities; Determining whether to establish or maintain an account, or to engage in a transaction; or assisting the financial institution in complying with any requirement of 31 C.F.R. Parts 1000 - 1009.

If, as a result of information shared, an RMLO knows, suspects, or has reason to suspect that an individual, entity, or organization is involved in, or may be involved in terrorist activity or money laundering, and such institution is subject to a suspicious activity reporting requirement, the institution shall file a SAR in accordance with those regulations. In situations involving violations requiring immediate attention, such as when a reportable violation involves terrorist activity or is ongoing, the RMLO shall immediately notify, by telephone, an appropriate law enforcement authority and RMLO supervisory authorities in addition to filing timely a SAR.

Examination Objectives and Procedures

Assess the adequacy of the company's reporting and recordkeeping procedures for the following:

- Suspicious Activity Reports (SARs)
- Form 8300 – Reports relating to currency in excess of $10,000
- Foreign Bank and Financial Accounts Reports (FBAR)
- International Transportation of Currency or Monetary Instruments (CMIR)
- Information Sharing 314(a) & 314(b)

Reporting Requirements Exam Procedures

	Examination Procedures	Y	N	Examiner Notes [Document supporting evidence and note determinations and findings made]
Suspicious Activity Reports – 31 CFR 1029.320				
1	• Review the company's policies and procedures for identifying and reporting suspicious activity. They should include: ○ Designation of individual responsible for compliance with 31 CFR			

	1029.320. ○ Monitoring systems and procedures used to identify unusual activity. ○ Procedures for documenting decisions not to file a SAR. ○ Procedures for completing and retaining supporting documentation. ○ Adequacy of confidentiality process.			
2	<u>Transaction Testing</u> On the basis of a risk assessment, prior examinations and independent testing findings, sample transactions and filed SARs to review the following: ○ SAR document contains accurate information. ○ SAR narratives are complete and explain clearly why the activity was considered suspicious. ○ 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. Select a sample of SARs that management decided not to file. Review if decision was reasonable and supported.			
Form 8300 – Currency in Excess of $10,000 – 31 CFR 1029.330				
3	The examiner should examine the appropriate documents and accounting records to determine: ○ Transaction involving the			

	receipt of reportable cash in excess of $10,000; ○ Consecutive or related reportable transactions in excess of $10,000; ○ Whether Form 8300 was filed on such transaction.			
4	The examiner should be alert to identifying transactions that may indicate attempts to avoid the 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.			
5	If a computerized system is utilized, the examiner must perform testing to ensure its integrity before relying upon such records for the Form 8300 compliance review.			
6	Depending on the initial findings of the Form 8300 compliance review, the examiner may need to expand the scope and/or depth of the review to include additional periods.			
7	Review procedures and select a sample from accounting records to determine cash handling and those transactions that are required to be filed on Form 8300.			

Foreign Bank and Financial Accounts Reporting (FBAR) (TD F90-223.1)				
8	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) (TD F 90-22.1) form. If applicable, review the bank's policies, procedures, and processes for filing annual reports.			
9	<u>Transaction Testing</u> On the basis of a risk assessment, prior examination reports, and a review of the company's examination findings, select a sample of accounts to determine whether the company has appropriately completed, submitted, and retained copies of the FBAR forms.			
10	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.			
International Transportation of Currency or Monetary Instruments Reporting				
11	Determine whether the bank has (or has caused to be) physically transported, mailed, or shipped currency or other monetary instruments in excess of $10,000, at one time, out of the United States, or whether the RMLO has received currency or other monetary instruments in excess of $10,000, at one time, that has been physically transported, mailed, or shipped			

	into the United States.			
12	If applicable, review the bank's policies, procedures, and processes for filing a Report of International Transportation of Currency or Monetary Instruments (CMIR) (FinCEN Form 105) for each shipment of currency or other monetary instruments in excess of $10,000 out of or into the United States (except for shipments sent through the postal service, common carrier, or to which another exception from CMIR reporting applies).			
13	<u>Transaction Testing</u> On the basis of a risk assessment, prior examination reports, and a review of the company's audit findings, select a sample of transactions conducted after the previous examination to determine whether the company has appropriately completed, submitted, and retained copies of the CMIR forms.			
14	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 CMIRs.			
15	On the basis of the previous conclusion and the risks associated with the company's activity in this area, proceed to expanded examination procedures, if necessary.			
Information Sharing Between Law Enforcement and Financial Institutions – Section 314(a) – 31 CFR 1029.520				
16	Verify that the company is currently receiving section			

	314(a) requests from FinCEN or from an affiliated company that serves as the subject company's point of contact. If the company is not receiving information requests or contact information changes, the company should update its contact information with its primary regulator, following the instructions at www.fincen.gov.			
17	Verify that the company has sufficient policies, procedures, and processes to document compliance; maintain sufficient internal controls; provide ongoing training; and independently test its compliance with 31 CFR § 1029.520, which implements section 314(a) of the 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.			
18	Determine whether the search policies, procedures, and processes the company uses to respond to section 314(a) requests are comprehensive and cover all records identified in the General Instructions for such requests. The General Instructions include searching accounts maintained by the			

	named subject during the preceding 12 months and transactions conducted within the last six months. The company has 14 days from the transmission date of the request to respond to a section 314(a) Subject Information Form.			
19	If the company uses a third-party vendor to perform or facilitate searches, determine whether an agreement or procedures are in place to ensure confidentiality.			
20	Review the company's internal controls and determine whether its documentation to evidence compliance with section 314(a) requests is adequate. This documentation could include, for example the following: o Copies of section 314(a) requests. o A log that records the tracking numbers and includes a sign-off column. o Copies of the cover page of the requests, with a financial institution sign-off, that the records were checked, the date of the search, and search results (e.g., positive or negative). For positive matches, copies of the form returned to FinCEN and the supporting documentation should be retained.			
Voluntary Information Sharing – Section 314(B) – 31 CFR 1029.540				
21	Determine whether the company has decided to share information voluntarily. If so, verify that the RMLO has filed a notification form with FinCEN and provides an effective date for the sharing of information that is within the previous 12 months.			

22	Verify that the company has policies, procedures, and processes for sharing information and receiving shared information, as specified under 31 CFR 1029.540, which implements section 314(b) of the Patriot Act.			
23	Companies that choose to share information voluntarily should have policies, procedures, and processes to document compliance; maintain adequate internal controls; provide ongoing training; and independently test its compliance. 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. If the company is sharing information with other entities and is not following the procedures, notify the examiners reviewing the privacy rules.			
24	Through a review of the company's documentation			

	(including loan files) on a sample of the information shared and received, evaluate how the company determined whether a Suspicious Activity Report (SAR) was warranted.			
Transaction Testing for 314(a)				
25	On the basis of a risk assessment, prior examination reports, and a review of the company's audit findings, select a sample of positive matches or recent requests to determine whether the following requirements have been met: ○ The company's policies, procedures, and processes enable it to search all of the records identified in the General Instructions for section 314(a) requests. Such processes may be electronic, manual, or both. ○ The RMLO searches appropriate records for each information request received. For positive matches: ▪ Verify that a response was provided to FinCEN within the designated time period (31 CFR 1010.520). ▪ Review the company's documentation (including account analysis) to evaluate how the company determined whether a SAR was warranted. RMLO are not required to file SARs solely on the basis of			

	a match with a named subject; instead, activity should be considered in determining whether a SAR is warranted.			
26	The RMLO uses information only in the manner and for the purposes allowed and keeps information secure and confidential (31 CFR 1010.520). *This requirement can be verified through discussions with management.*			
27	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 information sharing.			
28	Discuss items of concern, scope of work performed, and conclusions with the EIC.			
29	Organize and compile, if necessary, violations of law and regulation into a Violation Summary Sheet.			

Office of Foreign Assets Control (OFAC)

Overview & Exam Procedures

OFAC is an office of the U.S. Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against entities such as targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.

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 must review the RMLO's OFAC risk

assessment and independent testing to determine the extent to which a review should be conducted during the examination.

	Examination Procedures	Y	N	Examiner Notes [Document supporting evidence and note determinations and findings made]
1	Determine whether the RMLO has developed policies, procedures and processes to ensure compliance with OFAC.			
2	Determine the adequacy of independent testing and follow-up procedures.			
3	Sample new loans and evaluate how OFAC testing has been performed to ensure compliance.			
4	Review how the RMLO tests for OFAC and the blocking and rejection process.			

Definitions & Acronyms

Definitions

Financial Institution – Defined under BSA 31 USC 5312(a)(2) means:

(A) an insured bank (as defined in section 3(h) of the Federal Deposit Insurance Act (12 U.S.C. 1813(h)));
(B) a commercial bank or trust company;
(C) a private banker;
(D) an agency or branch of a foreign bank in the United States;
(E) any credit union;
(F) a thrift institution;
(G) a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.);
(H) a broker or dealer in securities or commodities;
(I) an investment banker or investment company;
(J) a currency exchange;
(K) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments;
(L) an operator of a credit card system;
(M) an insurance company;
(N) a dealer in precious metals, stones, or jewels;

(O) a pawnbroker;
(P) a loan or finance company;
(Q) a travel agency;
(R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system;
(S) a telegraph company;
(T) a business engaged in vehicle sales, including automobile, airplane, and boat sales;
(U) persons involved in real estate closings and settlements;
(V) the United States Postal Service;
(W) an agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph;
(X) a casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 which— (i) is licensed as a casino, gambling casino, or gaming establishment under the laws of any State or any political subdivision of any State; or (ii) is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act);
(Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or
(Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

Loan or finance company – a person engaged in activities that take place wholly or in substantial port within the United States in one or more of the capacities listed as a RMLO, whether or not on a regular basis or as an organized business concern. This includes but is not limited to maintenance of any agent, agency, branch, or office within the United State. For the purposes of this paragraph, the term “loan or finance company” shall include a sole proprietor acting as a loan or finance company, and shall not include (1) a bank, (2) a person registered with and functionally regulated or examined by the Securities and Exchange Commission of the Commodity Futures Trading Commission, (3) any government sponsored enterprise regulated by the Federal Housing Finance Agency, (4) any Federal or state agency or authority administering mortgage or housing assistance, fraud prevention or foreclosure prevention programs, or (5) an individual employed by a loan or finance company or

financial institution under this part. A loan or finance company is not a financial institution as defined in the regulations under at 31 CFR 1010.100(t).

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.

Residential mortgage loan – A loan that is secured by a mortgage, deed of trust, or other equivalent consensual security interest on (A) 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 (B) residential real estate upon which such a structure is constructed or intended to be constructed.

Residential mortgage originator – a person who accepts a residential mortgage loan application or offers or negotiates terms of a residential mortgage loan.

Acronyms

AML – Anti-money laundering program

BSA – The Bank Secrecy Act

FinCEN – Financial Crimes Enforcement Network, a bureau of the Department of the Treasury

RMLO- Residential mortgage lenders and originators which includes residential mortgage lender; residential mortgage originator; and residential mortgage loan.

SAR- Suspicious Activity Report

Secretary – Secretary of the Treasury