Anti-Money Laundering

Policies and Procedures

Senior Freedom Inc.

CONTENTS

ANTI-MONEY LAUNDERING POLICY AND PROCEDURES

This policy is adopted by Senior Freedom Inc. (hereinafter "SFI") in compliance with SFI's obligations under the Bank Secrecy Act ("BSA"), other related money laundering regulations, the requirements of the Financial Crimes Enforcement Network, along with federal and state licensing agencies.

On February 7, 2012, the Financial Crimes Enforcement Network (FinCEN), a bureau of the Dept of the Treasury, finalized regulations (Final Rule) requiring non-bank residential mortgage lenders and originators to establish anti-money laundering (AML) programs and file the same suspicious activity reports (SARs), as FinCEN requires of other types of financial institutions. FinCEN issued these regulations defining non-bank residential mortgage lenders and originators as loan or finance companies for the purpose of requiring them to establish anti-money laundering programs and report suspicious activities under the Bank Secrecy Act (BSA).

The final rule became effective 60 days after publication in the Federal Register. The effective compliance date for this final rule is August 13, 2012.

FinCEN may impose civil money penalties for noncompliance with the regulations, including $500 for each negligent currency transaction or suspicious activity reporting violation.* BSA authorizes the Secretary of the Treasury ("Secretary") to issue regulations requiring financial institutions, including any "loan or finance company" 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 counterintelligence activities, including analysis, to protect against international terrorism."

In the supplementary information to the Final Rule, the term 'loan or finance company' "can reasonably be construed to extend to any business entity that makes loans to or finances purchases on behalf of consumers and businesses. Some loan and finance companies extend personal loans and loans secured by real estate, mortgages and deeds of trust, including home equity loans."

Thus, the following constitutes the new definitions recognized by FinCEN:

Loan or Finance Company – A person engaged in activities that take place wholly or in substantial part within the United States in one or more of the capacities listed below, 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 States. The term "loan or finance company" shall include a sole proprietor acting as a loan or finance company, and shall not include: a bank, a person registered with and functionally regulated or examined by the SEC or the CFTC, any GSE regulated by the FHFA, any Federal or state agency or authority administering mortgage or housing assistance, fraud prevention or foreclosure prevention programs, or an individual employed by a loan or finance company or financial institution. A loan or finance company is not a financial institution as defined in these regulations.

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 Originator – The person accepting a residential mortgage loan application, or offers or negotiates terms of a residential mortgage loan.

Residential Mortgage Loan – The loan that is secured by a mortgage, deed of trust or other equivalent consensual security interest on:

- A residential structure that contains 1-4 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.

FinCEN interprets the term “loan or finance company” under the BSA to include any non-bank residential mortgage lender and/or originator (“RMLOs” – generally known as “mortgage companies” and “mortgage brokers” in the residential mortgage business sector).

SFI hereby acknowledges that it is a Residential Mortgage Lender and Originator.

The Board of Directors (“Board”), management, and staff of the Company are committed to implementing policies and procedures that assist in detecting and preventing money laundering or other illegal activities conducted through transactions within which the Company is involved.

RISK ASSESSMENT

The Board directs management to conduct an assessment of SFI’s overall risk for money laundering. The Board directs management to consider the following, when determining SFI’s risk for money laundering:

- The Company’s products and services
- The Company’s customers and the information learned about these customers
- The Company’s geographic locations and the locations of our customers

Management should follow all guidance offered by SFI’s federal regulator and the Financial Crimes Enforcement Network (FinCEN) concerning money laundering risks. The risk assessment should be updated from time to time but no less than every 18 months. Changes to SFI’s risk profile should be reported to the Board and internal controls to mitigate risk must be implemented.

THE MONEY LAUNDERING PROCESS

Money laundering is the criminal practice of filtering “ill-gotten gains” or “dirty” money through a maze or series of transactions, in an effort to “clean” these funds and make them appear to be proceeds from legal transactions. Money laundering does not always involve cash transactions at every stage of the money laundering process. Any transaction conducted with the Company has the potential to constitute money laundering.
Although money laundering is a diverse and often complex process, it involves three independent steps, which at times occur simultaneously:

- **Placement.** The process of placing, through deposits or other means, unlawful cash proceeds with traditional financial institutions.
- **Layering.** The process of separating the proceeds of criminal activity from their origin through the use of layers of complex financial transactions, such as converting cash into traveler’s checks, money orders, wire transfers, letters of credit, stocks, bonds, mortgages, or purchasing valuable assets, such as art or jewelry.
- **Integration.** The process of using an apparently legitimate transaction to disguise the illicit proceeds, allowing the laundered funds to be disbursed back to the criminal. Different types of financial transactions, such as sham loans or false import/export invoices, may be used.

POTENTIAL INDICATORS OF MONEY LAUNDERING

- Suspicious transactions that could be or appear to be linked to a common scheme.

ANTI-MONEY LAUNDERING DETECTION AND PREVENTION PROCEDURES

Monitoring for Suspicious Activity

The Board instructs management to institute procedures in each department which are designed to detect money laundering. Management is specifically directed to identify high-risk accounts in SFI’s pipeline using a federal banking agency's list or such other list of prohibited or restricted parties as a guide. In particular, management is

directed to perform diligent procedures on SFI's customers who are applying for a mortgage loan product, as defined by the BSA.

FinCEN is requiring that RMLOs establish AML programs and comply with SAR requirements. These AML programs are intended to cover initial purchase money loans and traditional refinancing transactions facilitated by RMLOs. Furthermore, FinCEN expects that RMLOs participating in transactions involving funds or programs under the Troubled Asset Relief Program and similar federal programs, or any similar state housing authority or housing assistance program to follow AML programs and file any necessary SARs to the extent that any transactions conducted by the RMLO could reasonably be considered to be extending a residential mortgage loan or offering or negotiating the terms of a residential mortgage loan.

In addition, the Board requires that management and the BSA Officer will ensure that the following reports are monitored for suspicious activity and that required employees receive adequate internal and external training on detecting money laundering and other illegal activities:

- **Delinquent loan reports.** Although these reports generally receive special attention, management is directed to pay close attention when delinquent loans are suddenly "cured" with no reasonable explanation in the file. Loan officers and underwriters must be able to explain a sudden payoff of seriously delinquent accounts.

- **Search Engines and Applications.** Management directs the use of the following search engines and applications on all residential mortgage loan originations in order to monitor for filing suspicious activity reports: LexisNexis, Interthinx, OFAC screens provided by Credit Reporting Agencies, and Mortgage Electronic Data Systems (MERS)**.**

Suspicious Activity Reporting

If any SFI employee becomes aware of, or suspects criminal activity by either SFI customers or employees, he or she should promptly report the matter to the BSA Officer or SFI president. The BSA Officer will promptly investigate the matter further to determine whether to report the suspicious activity to FinCEN. The investigation will be based on an objective review of the facts, as submitted by the employee, and a discussion with SFI officers in charge of the affected areas.

Supporting Documentation for the SAR

We will not include supporting documentation with the Suspicious Activity Report (SAR) when it is submitted to FinCEN, but will maintain all documentation that supports the facts and circumstances of the report in the SAR file either in hard copy or on computer disk, CD, or on anti-money laundering software.

Bank Secrecy Act Officer

Patrick O'Neil, SFI's Compliance Manager, is appointed as the anti-money laundering program coordinator ("BSA Officer") and is responsible for coordinating and monitoring day-to-day compliance with all federal and state laws relating to money laundering. It is the responsibility of the BSA Officer to coordinate and monitor day-to-day compliance with the detection and prevention of money laundering, including the training of Company employees.

Access to SAR Records

Retained records are kept in an electronic folder, marked "SAR Folder", and access to this retained records folder is strictly limited to the following employees of the Company:

- Patrick O'Neil, CEO

- Lawrence Berggoetz, President

Maintaining Accounts after a SAR Has Been Filed

The decision whether or not SFI will keep an account open after a SAR has been filed will be made by the BSA officer and may be made on a case-by-case basis. SFI will document the decision either to close or keep open the account in the SAR file.

If a law enforcement agency requests that SFI should maintain a particular account, SFI will ask for the request to be submitted in writing from a federal law enforcement agency. The request should be issued by a supervisory agent or by an attorney within a United States Attorney's Office or another office of the Department of Justice. If a state or local law enforcement agency requests that an account be maintained, then SFI will obtain a written request from a supervisor of the state or local law enforcement agency or from an attorney within our state or local prosecutor's office.

The written request should indicate that the agency has requested that SFI maintains the account and the purpose of the request. For example, if a state or local law enforcement agency is requesting that SFI maintain the account for purposes of monitoring, the written request should include a statement to that effect. The request should also indicate the duration for the request. The initial request should not exceed six (6) months. However, law enforcement may make additional requests for the maintenance of the same account after the expiration of the initial request.

Although there is no record keeping requirement under BSA for this type of correspondence, SFI will maintain documentation of such requests for at least five (5) years after the request has expired. If SFI is aware - through a subpoena, 314(a) request, National Security Letter, or similar communication - that an account is under investigation, SFI will notify law enforcement before making any decision regarding the status of the account.

Confidentiality

The BSA Officer and any other staff aware of the matter will keep the information confidential. SARs are also to be kept confidential. Any person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR shall decline to produce the information.

SFI will have in place a written confidentiality and internal control agreement regarding the handling of SARs, if at any time SFI becomes a subsidiary of a parent company. At such time as SFI becomes a subsidiary of a parent company, both SFI and the parent Company shall execute a Confidentiality and Internal Control Agreement that conforms to the Agreement specified in Appendix A herein. (See Appendix A: Confidentiality and Internal Control Agreement.)

If SFI determines it is necessary to report a suspected illegal activity, the BSA Officer will carefully review all known facts. SARs will only be filed when there is a reasonable basis for believing that a specific crime has occurred, is occurring, or may occur. Such reports will be filed with local agencies, and will take into consideration the provisions of the Right to Financial Privacy Act.

Regulators and Government Sponsored Entities

The following are SFI's regulatory agencies and Government Sponsored Entities:

FEDERAL REGULATORY ENTITIES

Consumer Financial Protection Bureau (CFPB)
Department of Housing and Urban Development (HUD)
Federal Reserve Board (FRB)
Federal Trade Commission (FTC)
Financial Crimes Enforcement Network (FinCEN)
Veterans Administration (VA)

STATE BANKING DEPARTMENTS

Texas

OVERSIGHT COMMITTEE

SARs will be reported to an Oversight Committee at each monthly meeting. The Oversight Committee consists of the following members:

- Lawrence Berggoetz

- Patrick O'Neil

TRAINING

The BSA Officer will conduct or arrange for annual meetings with all affected employees and other SFI personnel who handle any aspect of residential mortgage loan transactions to keep them informed of any new changes to the BSA or other related laws and updates to SFI's anti-money laundering procedures. It is also the responsibility of the BSA Officer to train all employees at the time of their initial employment. Additional meetings or other training will be held as necessary to address issues that arise in the interim.

Training may be conducted through presentations at a meeting, circulation of memoranda or other written materials, or any other appropriate manner. A copy of all materials presented or circulated shall be retained by the anti-money laundering program coordinator along with a written record of attendance or receipt by SFI personnel.

At least once per year, the BSA Officer will attend one external training session relating to the Bank Secrecy Act, fraud detection, or money laundering.

AUDIT PROCEDURES/INDEPENDENT TESTING

At least once each year, an independent audit of the procedures detailed in this policy will be conducted by an external auditor having no conflict of interest with SFI and entirely independent of the BSA Officer.

The results of the audit will be reported to the Board and the BSA Officer. It is the responsibility of the BSA Officer to take appropriate action to correct any problems found as a result of the audit and respond to the audit committee.

BOARD APPROVAL

The Board has approved and adopted this policy on June 6, 2014.

APPENDIX A: CONFIDENTIALITY AND INTERNAL CONTROL AGREEMENT

THIS AGREEMENT governs the disclosure of confidential information and internal controls surrounding Suspicious Activity Reports (SARs) by and between **Senior Freedom Inc. (SFI)** and a controlling or holding company. As of this update, SFI is not owned by a controlling entity or holding company. In the event that the SFI is owned by a controlling entity or holding company, this Appendix A will be executed.

Definition of Confidential Information

Confidential information means the actual SAR form and the fact that it has been filed with the Financial Crime Enforcement Network (FinCEN). It does not include the underlying information in the report, such as the name of the suspect or the suspicious transactions.

Sharing of Suspicious Activity Reports

From time to time, it may be necessary for **SFI** to share a copy of a SAR, or the fact that such a report has been filed with FinCEN, with the controlling entity or holding company. The circumstances under which such information will be shared are spelled out in the Company's Bank Secrecy Act and Anti-Money Laundering policy.

Internal Controls for Handling Suspicious Activity Reports

The controlling entity or holding company agrees that at all times and notwithstanding any termination or expiration of this agreement it will hold in strict confidence and not disclose to any third party information from the SAR or the fact that a SAR has been filed. The controlling entity or holding company shall only permit access to SARs to those of its employees or authorized representatives having a need to know.

The controlling entity or holding company will implement the appropriate internal controls necessary to maintain the confidentiality of the SARs of SFI.

IN WITNESS WHEREOF, the parties hereto have caused this confidentiality agreement to be executed as of the effective date.

For: Parent or Controlling Company

_____

By: Name _____

Title _____

Date_____

For: Senior Freedom, Inc.

_____

By: Name _____

Title _____

Date _____

APPENDIX B: REGISTERING FOR ELECTRONIC FILING

The following outline provides the registration procedures for E-Filing

Why is FinCEN mandating E-Filing?

The Financial Crimes Enforcement Network (FinCEN) is requiring the electronic filing of certain FinCEN reports. Additionally, BSA E-Filing allows organizations or individuals to electronically and securely file discrete and batched FinCEN reports. It also allows a registered user to send secure messages to FinCEN (and receive responses where appropriate).

When did FinCEN decide to make E-Filing mandatory?

Final Notice mandating E-Filing was issued by FinCEN on February 24, 2012. [Final Notice, 77 Federal Register 12367 (2012)]

E-Filing is mandatory as of July 1, 2012.

What steps must be taken to register for E-Filing?

1. Visit the BSA E-Filing System.

2. Click **Become a BSA E-Filer** and follow the instructions in order to enroll as a Supervisory User in BSA E-Filing.

3. The enrollment process can take from five to seven days.

Is there a cost to participating in BSA E-Filing?

No, the BSA E-Filing system is free.

When does E-Filing become mandatory?

With limited exceptions, E-Filing is mandatory effective July 1, 2012.

What FinCEN Reports must be E-Filed?

Suspicious Activity Reports must be filed beginning August 13, 2012.

Where can I find more information about BSA E-Filing?

- For more information about BSA E-Filing: review the E-Filing Section on FinCEN's Website.

- Technology related questions specific to E-Filing: call the BSA E-Filing Help desk at 1-866- 346-9478.

- FinCEN has additionally prepared an instructional presentation on how to file electronically.

APPENDIX C: REQUIRED REPORTING

Every RMLO shall file with FinCEN a report of any suspicious transaction relevant to a possible violation of law or regulation. An RMLO may also file with FinCEN a report of any suspicious transaction that it believes is relevant to the possible violation of any law or regulation, but whose reporting is not required.

Required Reporting

A transaction requires reporting if it is conducted or attempted by, at, or through an RMLO if it involves or aggregates funds or other assets of at least $5,000, and the RMLO knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

1. Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;

2. Is designed, whether through structuring or other means, to evade any requirements of this part or any other regulations promulgated under the BSA;

3. 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; or,

4. Involves use of the RMLO to facilitate criminal activity.

Reporting Same Transactions

More than one RMLO may have an obligation to report the same transaction, and other financial institutions may have separate obligations to report suspicious activity with respect to the same transaction. In those instances, no more than one report is required to be filed by the RMLO and other financial institution(s) involved in the transaction.

Timing for filing SAR Reports

A SAR shall be filed no later than 30 calendar days after the date of the initial detection by the reporting RMLO of facts that may constitute a basis for filing a SAR. If no suspect is identified on the date of such initial detection, an RMLO may delay filing a SAR for an additional 30 calendar days to identify a suspect, but in no case shall reporting be delayed more than 60 calendar days after the date of such initial detection.

In situations involving violations that require immediate attention, such as suspected terrorist financing or ongoing money laundering schemes, a loan or finance company shall immediately notify by telephone an appropriate law enforcement authority in addition to filing timely a SAR.

Record Retention

SAR Reports must be retained for 5 years from the date of filing.

APPENDIX D: AML PROGRAM REQUIREMENTS

Minimum Requirements RMLOs†

§ 1029.210 Anti-money laundering programs for loan or finance companies.

(a) Anti-money laundering program requirements for loan or finance companies. Each loan or finance company shall develop and implement a written anti-money laundering program that is reasonably designed to prevent the loan or finance company from being used to facilitate money laundering or the financing of terrorist activities. The program must be approved by senior management. A loan or finance company shall make a copy of its anti-money laundering program available to the Financial Crimes Enforcement Network or its designee upon request.

(b) Minimum requirements. At a minimum, the anti-money laundering program shall:

(1) Incorporate policies, procedures, and internal controls based upon the loan or finance company's assessment of the money laundering and terrorist financing risks associated with its products and services. Policies, procedures, and internal controls developed and implemented by a loan or finance company under this section shall include provisions for complying with the applicable requirements of subchapter II of chapter 53 of title 31, United States Code and this part, integrating the company's agents and brokers into its anti-money laundering program, and obtaining all relevant customer-related information necessary for an effective anti-money laundering program.

(2) Designate a compliance officer who will be responsible for ensuring that:

(i) The anti-money laundering program is implemented effectively, including monitoring compliance by the company's agents and brokers with their obligations under the program;

(ii) The anti-money laundering program is updated as necessary; and

(iii) appropriate persons are educated and trained in accordance with paragraph (b)(3) of this section.

(3) Provide for on-going training of appropriate persons concerning their responsibilities under the program. A loan or finance company 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 loan or finance company.

(4) Provide for independent testing to monitor and maintain an adequate program, including testing to determine compliance of the company's agents and brokers with their obligations under the program. 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 any officer or employee of the loan or finance company, other than the person designated in paragraph (b)(2) of this section.

(c) Compliance. Compliance with this section shall be examined by FinCEN or its delegates, under the terms of the Bank Secrecy Act. Failure to comply with the requirements of this section may constitute a violation of the Bank Secrecy Act and of this part. (d) Compliance date. A loan or finance company must develop and implement an anti-money laundering program that complies with the requirements of this section by August 13, 2012.

APPENDIX E: EXAMINATION AND ENFORCEMENT

Initially, the Internal Revenue Service has the delegated authority to examine for compliance with FinCEN's regulations since RMLOs do not have a federal function regulator.

FinCEN has announced that it will consider whether other state and federal agencies, such as the Consumer Financial Protection Bureau and the Federal banking agencies, should also have examination authority.

If FinCEN further delegates examination authority, it has stated its commitment to work with the other relevant regulatory agencies to develop consistent examination procedures.

APPENDIX F: RED FLAGS (FFIEC)

Appendix F: Money Laundering and Terrorist Financing "Red Flags" of the Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/ Anti-Money Laundering Examination Manual provides the following Red Flags.§ This list is not meant to be comprehensive and it is expected to be updated from time to time. It reflects the types of transactions that usually involved the Company as an RMLO.

The following are examples of potentially suspicious activities, or "red flags" for both money laundering and terrorist financing. Although these lists are not all-inclusive, they may help banks and examiners recognize possible money laundering and terrorist financing schemes. Management's primary focus should be on reporting suspicious activities, rather than on determining whether the transactions are in fact linked to money laundering, terrorist financing, or a particular crime.

The following examples are red flags that, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny should help to determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose.

POTENTIALLY SUSPICIOUS ACTIVITY THAT MAY INDICATE MONEY LAUNDERING

Customers Who Provide Insufficient or Suspicious Information

- A customer uses unusual or suspicious identification documents that cannot be readily verified.

- A customer provides an individual tax identification number after having previously used a Social Security number.

- A customer uses different tax identification numbers with variations of his or her name.

- A business is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location.

- A customer's home or business telephone is disconnected.

- The customer's background differs from that which would be expected on the basis of his or her business activities.

- A customer makes frequent or large transactions and has no record of past or present employment experience.

- A customer is a trust, a shell company, or Private Investment Company that is reluctant to provide information on controlling parties and underlying beneficiaries. Beneficial owners may hire nominee incorporation services to establish shell companies and open bank accounts for those shell companies while shielding the owner's identity.

Efforts to Avoid Reporting or Record keeping Requirement

- A customer or group tries to persuade an employee not to file required reports or maintain required records.

- A customer is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.

- A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.

- A business or customer asks to be exempted from reporting or recordkeeping requirements.

- A person customarily uses the automated teller machine to make several bank deposits below a specified threshold.

- A customer deposits funds into several accounts, usually in amounts of less than $3,000, which are subsequently consolidated into a master account and transferred outside of the country, particularly to or through a location of specific concern (e.g., countries designated by national authorities and Financial Action Task Force on Money Laundering (FATF) as non-cooperative countries and territories).

- A customer accesses a safe deposit box after completing a transaction involving a large withdrawal of currency, or accesses a safe deposit box before making currency deposits structured at or just under $10,000, to evade CTR filing requirements.

Funds Transfers

- Many funds transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts.

- Funds transfer activity occurs to or from a financial secrecy haven, or to or from a higher-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.

- Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.

- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.

- Funds transfer activity is unexplained, repetitive, or shows unusual patterns.

- Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.

- Funds transfers are sent or received from the same person to or from different accounts.

- Funds transfers contain limited content and lack related party information.

Automated Clearing House Transactions

- Large-value, automated clearing house (ACH) transactions are frequently initiated through third-party service providers (TPSP) by originators that are not bank customers and for which the bank has no or insufficient due diligence.

- TPSPs have a history of violating ACH network rules or generating illegal transactions, or processing manipulated or fraudulent transactions on behalf of their customers.

- Multiple layers of TPSPs that appear to be unnecessarily involved in transactions.

- Unusually high level of transactions initiated over the Internet or by telephone.

- NACHA — The Electronic Payments Association (NACHA) information requests indicate potential concerns with the bank's usage of the ACH system.

Activity Inconsistent with the Customer's Business

- The currency transaction patterns of a business show a sudden change inconsistent with normal activities.

- A large volume of cashier's checks, money orders, or funds transfers is deposited into, or purchased through, an account when the nature of the accountholder's business would not appear to justify such activity.

- A retail business has dramatically different patterns of currency deposits from similar businesses in the same general location.

- Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.

- The owner of both a retail business and a check-cashing service does not ask for currency when depositing checks, possibly indicating the availability of another source of currency.

- Goods or services purchased by the business do not match the customer's stated line of business.

- Payments for goods or services are made by checks, money orders, or bank drafts not drawn from the account of the entity that made the purchase.

Lending Activity

- Loans secured by pledged assets held by third parties unrelated to the borrower.

- Loan secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.

- Borrower defaults on a cash-secured loan or any loan that is secured by assets which are readily convertible into currency.

- Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.

- To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments.

- Loans that lack a legitimate business purpose, provide the company with significant fees for assuming little or no risk, or tend to obscure the movement of funds (e.g., loans made to a borrower and immediately sold to an entity related to the borrower).

POTENTIALLY SUSPICIOUS ACTIVITY THAT MAY INDICATE TERRORIST FINANCING

The following examples of potentially suspicious activity that may indicate terrorist financing are primarily based on guidance "Guidance for Financial Institutions in Detecting Terrorist Financing" provided by the FATF.269 FATF is an intergovernmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. Guidance for Financial Institutions in Detecting Terrorist Financing is available at www.fatf-gafi.org.

Activity Inconsistent with the Customer's Business

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and FATF as non-cooperative countries and territories).

- The stated occupation of the customer is not commensurate with the type or level of activity.

- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).

- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

Funds Transfers

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.

- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.

- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.

- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.

Other Transactions That Appear Unusual or Suspicious

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.

- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.

- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.

- Banks from higher-risk locations open accounts.

- Funds are sent or received via international transfers from or to higher-risk locations.

- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

APPENDIX G: RED FLAGS – IDENTITY THEFT PREVENTION

26 RED FLAGS: INTERAGENCY GUIDANCE

1. A fraud alert included with a consumer report.

2. Notice of a credit freeze in response to a request for a consumer report.

3. A consumer reporting agency providing a notice of address discrepancy.

4. Unusual credit activity, such as an increased number of accounts or inquiries.

5. Documents provided for identification appearing altered or forged.

6. Photograph on ID inconsistent with appearance of customer.

7. Information on ID inconsistent with information provided by person opening account.

8. Information on ID, such as signature, inconsistent with information on file at financial institution.

9. Application appearing forged or altered or destroyed and reassembled.

10. Information on ID not matching any address in the consumer report, Social Security number has not been issued or appears on the Social Security Administration's Death Master File.

11. Lack of correlation between Social Security number range and date of birth.

12. Personal identifying information associated with known fraud activity.

13. Suspicious addresses supplied, such as a mail drop or prison, or phone numbers associated with pagers or answering service.

14. Social Security number provided matching that submitted by another person opening an account or other customers.

15. An address or phone number matching that supplied by a large number of applicants.

16. The person opening the account unable to supply identifying information in response to notification that the application is incomplete.

17. Personal information inconsistent with information already on file at financial institution or creditor.

18. Person opening account or customer unable to correctly answer challenge questions.

19. Shortly after change of address, creditor receiving request for additional users of account.

20. Most of available credit used for cash advances, jewelry or electronics, plus customer fails to make first payment.

21. Drastic change in payment patterns, use of available credit or spending patterns.

22. An account that has been inactive for a lengthy time suddenly exhibits unusual activity.

23. Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account.

24. Financial institution or creditor notified that customer is not receiving paper account statements.

25. Financial institution or creditor notified of unauthorized charges or transactions on customer's account.

26. Finance institution/creditor notified that it has opened a fraudulent account for person engaged in identity theft.

APPENDIX H: TRAINING OUTLINE

Course Outline

External training

- Money Laundering and Terrorist Financing
- Red Flags
- The Bank Secrecy Act
- The USA PATRIOT Act
- Government Agencies
- Suspicious Activity Reporting Requirement
- Money Laundering Typologies
- Completing a SAR
- Customer Identification Program
- Risk Management Through Customer Due Diligence

Learning Objectives

 Gain an understanding of money laundering and terrorist financing and their adverse effects on mortgage professionals, including a review of associated red flags

 Explore the Bank Secrecy Act, including a brief history, objectives, coverage, requirements, and penalties

 Briefly take a look at the USA PATRIOT Act, specifically its coverage in relation to the mortgage profession

 Examine the role of government agencies in the prevention of money laundering

 Review the requirements for an appropriate compliance program, including the requirement to report large currency transactions

 Take a look at Suspicious Activity Report requirements

 Explore the need for a Customer Identification Program, including requirements and methods for properly identifying customers

 Analyze subjects such as risk management and information sharing

Other Methodologies

Webinars conducted by FinCEN and continuing education vendors.

APPENDIX I: PROCEDURES AND TIMING OF THE SAR

SAR completion and filing are a critical part of the SAR monitoring and reporting process. Appropriate policies, procedures, and processes are in place to ensure SAR forms are filed in a timely manner, are complete and accurate, and that the narrative provides a sufficient description of the activity reported as well as the basis for filing.

The SAR rules require that a SAR be filed 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 can be identified, the time period for filing a SAR is extended to 60 days.

The Company may need to review transaction or account activity for a customer to determine whether to file a SAR. The need for a review of customer activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the Company, 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 phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an account holder’s normal account activity. For example, a real estate investment (purchase or sale), the receipt of an inheritance, or a gift, may cause an account to be inconsistent with typical account activity.

The Company’s automated methodologies or initial discovery of information, such as system- generated reports and employee notification, may flag the transaction; however, this should not be considered initial detection of potential 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.

Whenever possible, an expeditious review of the transaction or the account is recommended and can be of significant assistance to law enforcement. In any event, the review should be completed in a reasonable period of time. What constitutes a "reasonable period of time" will vary according to the facts and circumstances of the

particular matter being reviewed and the effectiveness of the SAR monitoring, reporting, and decision-making process of each bank. The key factor is that the Company has established adequate procedures for reviewing and assessing facts and circumstances identified as potentially suspicious, and that those procedures are documented and followed.

For situations requiring immediate attention, in addition to filing a timely SAR, the Company must immediately notify, by telephone, an "appropriate law enforcement authority" and, as necessary, the Company's primary regulator. For this initial notification, an "appropriate law enforcement authority" would generally be the local office of the IRS Criminal Investigation Division or the FBI. Notifying law enforcement of a suspicious activity does not relieve the Company of its obligation to file a SAR.

APPENDIX J: PROHIBITION OF SAR DISCLOSURE

No director, officer, employee, or agent of SFI that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. Thus, any person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR, except when such disclosure is requested by FinCEN or an appropriate law enforcement or federal banking agency, shall decline to produce the SAR or to provide any information that would disclose that a SAR has been prepared or filed.

FinCEN and SFI's regulator should be notified of any such request and of SFI's response. Furthermore, FinCEN and the Company's regulator take the position that the Company's internal controls for the filing of SARs should minimize the risks of disclosure.

Sharing SARs with Head Offices and Controlling Companies

Interagency guidance clarifies that financial institutions may share SARs with head offices and controlling companies, whether located in the United States or abroad.

A controlling company as defined in the FinCEN guidance includes:

- A bank holding company (BHC), as defined in section 2 of the BHC Act.
- A savings and loan holding company, as defined in section 10(a) of the Home Owners' Loan Act.
- A company having the power, directly or indirectly, to direct the management policies of a Residential Mortgage Lender or Originator or a parent company or to vote 25 percent or more of any class of voting shares of a Residential Mortgage Lender or Originator or parent company.

FinCEN guidance confirms that:

- A U.S. Residential Mortgage Lender or Originator may share a SAR with its head office outside the United States.
- A U.S. Residential Mortgage Lender or Originator may share a SAR with controlling companies whether domestic or foreign.

SFI maintains appropriate arrangements to protect the confidentiality of SARs.

FinCEN guidance does not address whether a Residential Mortgage Lender or Originator may share a SAR with an affiliate other than a controlling company or head office. However, in order to manage risk across the Company, SFI has determined that when a SAR is filed, the information underlying a SAR filing may be disclosed to the BSA officer of an affiliate.

APPENDIX K: SAR DECISION MAKING

After thorough research and analysis has been completed, findings are typically forwarded to a final decision maker (individual or committee). SFI has policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management has established a clear and defined escalation process from the point of initial detection to disposition of the investigation.

The “decision maker”, either an individual or committee, should have the authority to make the final SAR filing decision. When SFI uses a committee, there is a clearly defined process to resolve differences of opinion on filing decisions.

SFI documents 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. However, due to the variety of systems used to identify, track, and report suspicious activity, as well as the fact that each suspicious activity reporting decision will be based on unique facts and circumstances, no single form of documentation is required when SFI decides not to file.

The decision to file a SAR is an inherently subjective judgment. During banking examinations SFI recognizes that the Examiner will focus on whether SFI 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 SFI has an established SAR decision-making process, has followed existing policies, procedures, and processes, and has determined not to file a SAR, SFI does not expect to be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.

SAR Filing on Continuing Activity

One purpose of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This objective is accomplished by the filing of a SAR that identifies the activity of concern. If this activity continues over a period of time, such information should be made known to law enforcement and the federal banking agencies.

FinCEN’s guidelines suggest that a financial institution should report continuing suspicious activity by filing a report at least every 90 days. This practice will notify law enforcement of the continuing nature of the activity in aggregate. In addition, this practice acts as a reminder to SFI that it should continue to review the suspicious activity to determine whether other actions may be appropriate, such as management determining that it is necessary to terminate a relationship with the customer or employee that is the subject of the filing.

SFI is aware that law enforcement may have an interest in ensuring that certain accounts remain open notwithstanding suspicious or potential criminal activity in connection with those accounts. If a law enforcement agency requests that the Company maintain a particular account, SFI shall ask for a written request. The written request shall indicate that the requesting agency has requested that SFI maintain the account and the purpose and duration of the request. Ultimately, the decision to maintain or close an account will be made by SFI in accordance with its own standards and guidelines.

SFI has policies, procedures, and processes indicating when to escalate issues or problems identified as the result of repeat SAR filings on accounts.

The Company’s procedures include:

- Review by senior management and legal staff (i.e., BSA Officer or SAR committee).
- Criteria for when analysis of the overall customer relationship is necessary.
- Criteria for whether and, if so, when to close the account.
- Criteria for when to notify law enforcement, if appropriate.

APPENDIX L: IDENTIFYING THE UNDERLYING CRIME

SFI is not required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing, and certain other crimes above prescribed dollar thresholds.

SFI is not obligated to investigate or confirm the underlying crime (i.e., terrorist financing, money laundering, tax evasion, identity theft, and various types of fraud).

Investigation is the responsibility of law enforcement.

When evaluating suspicious activity and completing the SAR, SFI shall, to the best of its ability, identify the characteristics of the suspicious activity.

APPENDIX M: SAFE HABOR FROM LIABILITY

Federal law 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.

Specifically, the law provides that a financial institution 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."

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.

APPENDIX N: IDENTIFY, RESEARCH, REPORT

This Anti-Money Laundering policy statement contains several methodologies to identify and research suspicious activity. Suspicious activity monitoring and reporting are critical internal controls. Proper monitoring and reporting processes are essential to ensuring that SFI has an adequate and effective BSA compliance program.

Appropriate policies, procedures, and processes are in place to monitor and identify unusual activity. The sophistication of monitoring systems is dictated by SFI's risk profile, with particular emphasis on the composition of higher-risk products, services, customers, entities, and geographies. SFI ensures adequate staff to the identification, research, and reporting of suspicious activities, taking into account SFI's overall risk profile and the volume of transactions. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or any combination of these.

Generally, effective suspicious activity monitoring and reporting systems include four key components. 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 compliance.

The four key components to an effective monitoring and reporting system are:

- Identification or alert of unusual activity (which may include: employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output).
- Managing Alerts (see Appendix O)
- SAR Decision Making (see Appendix K)
- SAR completion and filing (See Appendix I)

These four components are present in financial institutions of all sizes. However, the structure and formality of the components may vary.

Larger Residential Mortgage Lenders or Originators will typically have greater differentiation and distinction between functions, and may devote entire departments to the completion of each component. Smaller Residential Mortgage Lenders or Originators may use one or more employees to complete several tasks (i.e., review of monitoring reports, research activity, and completion of the actual SAR).

This Company's Anti-Money Laundering policies, procedures, and processes describe the steps it 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, and SAR completion and filing.

The following flow chart outlines the appropriate organizational flow of information:

KEY SUSPICIOUS ACTIVITY MONITORING COMPONENTS:

Identification of Unusual Activities

Employee Identification
Law Enforcement inquiries
Other referrals
Transactions
And surveillance monitoring systems

Alert Management

SAR Decision Making

SAR Completion and Filing

APPENDIX O: MANAGING ALERTS

Alert management focuses on processes used to investigate and evaluate identified unusual activity. SFI is aware of the most prominent methods used by Residential Mortgage Lenders or Originators to identify and ensure that its suspicious activity monitoring program includes processes to evaluate any unusual activity identified, regardless of the method of identification.

SFI has policies, procedures, and processes in place for referring unusual activity from all areas of SFI or business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management has established a clear and defined escalation process from the point of initial detection to disposition of the investigation.

SFI has assigned adequate staff to the identification, evaluation, and reporting of potentially suspicious activities, taking into account SFI's overall risk profile and the volume of transactions. Additionally, SFI has ensured that assigned the staff possess the requisite experience levels and are provided with comprehensive and ongoing training to maintain their expertise. Staff is also provided with sufficient internal and external tools to allow them to properly research activities and formulate conclusions.

Internal research tools include, but are not limited to, the methodologies outlined in this Anti-Money Laundering policy statement. External research tools may include widely available Internet media search tools, as well those accessible by subscription. After thorough research and analysis, investigators should document conclusions including any recommendation regarding whether or not to file a SAR.

When multiple departments are responsible for researching unusual activities (i.e., the BSA department researches BSA-related activity and the Fraud department researches fraud-related activity), the lines of communication between the departments shall remain open. This allows SFI, when multiple processes are present, to gain efficiencies by sharing information, reducing redundancies, and ensuring all suspicious activity is identified, evaluated, and reported.

If applicable, reviewing and understanding suspicious activity monitoring across SFI branches, affiliates, subsidiaries, and business lines enhances SFI's ability to detect suspicious activity, and thus minimize the potential for financial losses, increased legal or compliance expenses, and reputational risk to the organization. Refer to the expanded overview section.

APPENDIX P: COMMON FILING ERRORS

The Financial Crimes Enforcement Network ("FinCEN") has noticed common errors in the filing of Suspicious Activity Reports ("SARs"). Although these errors were noted primarily through studying Suspicious Activity Reports by Money Services Business (Form 109) filings, FinCEN believes that publishing an explanation of ten of the most common errors and ways much of them readily can be mitigated could be informative to financial institutions in other industries in their efforts to implement simple strategies to provide accurate and complete information in their SAR filings.

We expects that SAR filers who are trained on the requirements would already have available the information necessary to complete the SAR properly, meaning that significant improvements to the SAR filing could be made without significant additional efforts beyond those already undertaken for the investigation and decision to file a SAR which may contain errors.

It is critical that the information provided in a SAR filing be as accurate and complete as possible. SAR information provides a valuable tool to FinCEN, law enforcement, regulatory authorities, and intelligence agencies (collectively referred to as "users"), allowing the observation of larger patterns of suspicious activity, which might not have otherwise been detected. When combined with other sources, the information generated from SAR filings also plays an important role for law enforcement agencies in identifying potentially illegal activities, such as money laundering and terrorist financing, and assists in detecting and preventing the flow of illicit funds through our financial system.

FinCEN has identified three areas where financial institutions should concentrate efforts to ensure information contained in the SAR is complete:

(1) SAR narratives,

(2) Certain critical fields that allow users to analyze quickly where activity has occurred, and

(3) Fields that identify the type, category and character of the suspicious activity.

(1) The Importance of Complete SAR Narratives

In general, an accurate and complete SAR narrative should identify the five essential elements - **who? what? when? where?** and **why?** of the suspicious activity being reported. SAR narratives should describe, as fully as possible, why the activity or transaction is unusual for the customer, taking into consideration the types of products and services offered by your industry and the nature and typical activities of similar customers. Explaining why the transaction is suspicious is critical. The following are common responses received in the SAR narrative field, which does not allow users to fully utilize the information submitted.

Empty Narrative Field: The narrative field in the form must explain why the transaction was suspicious. If the narrative field is left blank, the information in the SAR only addresses the "who/what/when/where" of the transaction. Each SAR filing must have a narrative that accurately explains the nature and circumstances of the suspicious activity. Otherwise, the information contained in the SAR is of limited utility.

Failure to Explain Information in Supporting Documents: All SAR Form Instructions specifically state that the attachment of supporting documentation is prohibited. Supporting documents cannot be uploaded into the database and should not be used as a substitute for the narrative, since law enforcement, FinCEN and other intelligence agencies cannot readily view the documents or the information contained therein. The information appearing in any such supporting documentation should be reasonably described in the narrative and must be maintained for five years to be made available upon specific request.

Inadequate Narratives: Any narrative that does not accurately and completely explain the nature and circumstances of the suspicious activity is an inadequate narrative. In general, most inadequate narratives merely repeat data in the form's fixed fields (for example, "John Doe sent two money transfers on 1/1/2007.", or "Wired $2,000 to Mexico."). Restating the information found in critical fields does not sufficiently illustrate why the transaction was suspicious, considering the nature and expected activities of the institution's customers.

(2) Responses in Fields of Critical Value

The responses provided in fields of critical value, marked by an asterisk (*) in most SAR forms, are examined by users to track activity and follow-up on leads provided in SARs. This information is also used by FinCEN to develop analytical products that are distributed to law enforcement, regulators and other intelligence agencies, as well as to provide general feedback to financial institutions. The quality of this information is of utmost importance: when inaccurate or incomplete information is provided, its utility is diminished significantly. Several common issues arising from reports including inaccurate or incomplete information in critical fields are listed immediately below.

Inaccurate Special Responses: As noted in the instructions to the SAR forms, specific responses are required when data is unavailable. Institutions should not create their own responses. Special responses (for example, "N/A" or "Same as above") pose as real data and distort statistics on how often certain items of data are unavailable. It is extremely important that reporting institutions follow the instructions on the form and input the proper responses for unavailable information.

Missing or Incomplete Filer Employer Identification Number ("EIN"): The EIN of the reporting institution permits regulators and law enforcement to follow transactions properly through entities that report them. A reporting institution is expected to know its EIN and report it accurately. Invalid or incomplete entries are unacceptable. EIN entries of "000000000" and "999999999" are examples of invalid entries. Incomplete EINs have fewer than nine digits and are usually the result of the preparer entering the EIN with a hyphen in a nine-digit fill-in field, causing the last digit of the number to disappear. Incomplete entries are also created by typographical errors that were not caught in review.

Missing Filer Telephone Number: SAR information users must have the ability to contact the reporting financial institution to follow up on any leads relating to possible criminal activity. The telephone numbers of the financial institution, including the specific transaction location, are critical for this reason, and must be included in any SAR filing. To reiterate, hyphens should not be included in the critical fields.

Invalid Subject Social Security Number ("SSN")/EIN: The SAR forms and the E-filing manual provide specific instructions regarding acceptable entries in the SSN/EIN fields when the respective number is unknown. Consult the form instructions or the E-filing instructions when completing these sections. Entries of "000000000" and "999999999" are examples of invalid entries that cause an inaccurate record of the activity, which is of no value to those who utilize SAR information.

Incomplete Subject Information; Government Issued Identification: The method used to identify the subject should be as complete as possible. A driver's license or passport provides law enforcement with the information necessary to find out who a subject is and where a subject may be located. The exclusion of an identification number when the issuer is known is an example of a commonly received incomplete response. If a government issued identification card or document was used during the transaction, then both the number and issuer of the identification card or document should be provided.

(3) Identifying the Category and Character of Suspicious Activity

By filling out SARs as accurately and completely as possible, financial institutions help mitigate their risk by maintaining a strong component of their anti-money laundering ("AML") programs. Employee training in the recognition of suspicious activity and the proper filing of SARs protects the financial institution and aids law enforcement in apprehending criminals.*** The following are common responses received in the SAR fields which identify the type of suspicious activity. The lack of accurate and complete information addressed below hinders the usage of SAR information.

Missing Category, Type, or Characterization of Suspicious Activity: It is important for users to know why the activity is being reported and how the activity may relate to ongoing investigations. The category, type, or characterization of suspicious activity is important in this regard. This field should never be blank. If none of the available options appear to apply to the particular activity that is being reported, then the "other" box should be checked, and a brief and informative description should be entered in the "other" text field, if provided, or in the narrative.

Incorrect Characterization of Suspicious Activity: In order to provide accurate information to all users, FinCEN reviews narratives and other SAR data to verify that the category of suspicious activity appears correct. Many times, the characterization of suspicious activity appears incorrect or has not been selected. In these cases, there is no information in the SAR to substantiate the checked selections. For example, an institution may report that a customer comes in frequently to purchase monetary instruments below the $3,000 recordkeeping threshold, indicating the potential that the customer could be "structuring" transactions; however, the narrative does not provide any information about previous transactions, and there are no prior SARs filed on the subject of the SAR.

Conclusion

When accurate and complete, SARs are an important tool in combating financial crimes. When completed correctly, the forms provide its users with important information that can be used to analyze broad sets of data and to apprehend suspected criminals and terrorists. When the SAR forms are filled out incorrectly or are incomplete, they generally do not provide useful and adequate information, and in some cases, distort information reviewed by FinCEN and other users. Further, by filling out SARs as accurately and completely as possible, financial institutions also maintain a picture of the identified, suspicious transactions flowing through them, which may be of use in their AML program for risk mitigation purposes.

FinCEN has offered some simple suggestions that may reduce incomplete and/or incorrect SARs. As AML programs are designed on a risk-basis by financial institutions to meet their own specific needs, some of the following suggestions may not be directly applicable to the way that the Company conducts business.

1. Sign up for BSA E-filing. This will eliminate errors of omission because preparers must enter the required data or a special response in critical fields. Information on signing up for E-filing can be found on www.fincen.gov by clicking on "BSA E-filing" or by calling 1- 888-827-2778 (option 6).

2. Provide staff and preparers with training on recognizing suspicious activity and avoiding SAR filing errors. This training will help the financial institution maintain an effective AML compliance program, as well as protect the institution from potential abuse by criminals.

3. Provide preparers with examples of accurate and complete SAR filings with "John Doe" data in the fields. This will allow preparers to see the correct format of a completed SAR form and can serve as a reference point for future filings. Please ensure that these sample or mock forms are not filed with FinCEN.

4. Ensure that preparers know the company EIN, address, telephone number, contact office, etc., for the Reporting Business and Contact for Assistance fields. This will allow the preparers to provide FinCEN with accurate reporting information; as well, it provide law enforcement with accurate contact information should further investigation be required.

5. Provide preparers with the instructions for completing the form currently in use. When a new form is released, do not rely on old instructions and training because there likely will be significant changes. While form changes are infrequent, being up-to-date on the most current forms helps financial institutions with their regulatory compliance requirements and enables them to provide FinCEN and other users with the most accurate data possible.

6. Provide preparers with the FinCEN Regulatory Helpline number, (800) 949-2732, the FinCEN homepage, www.fincen.gov.

7. Have a second reviewer to ensure accuracy and completeness. An additional review of the SAR will help to eliminate errors and omissions.

APPENDIX Q: SAR NARRATIVE

In general, a SAR narrative should identify the five essential elements of information – **who? what? when? where? and why?** of the suspicious activity being reported. The method of operation (or how?) is also important and should be included in the narrative. (see Appendix P)

Who is conducting the suspicious activity?

While one section of the SAR form calls for specific suspect information, the narrative should be used to further describe the suspect or suspects, including occupation, position or title within the business, and the nature of the suspect's business(es). If more than one individual or business is involved in the suspicious activity, identify all suspects and any known relationships amongst them in the Narrative Section. While detailed suspect information may not always be available (i.e., in situations involving non-account holders), such information should be included to the maximum extent possible. Addresses for suspects are important: filing institutions should note not only the suspect's primary street addresses, but also, other known addresses, including any post office box numbers and apartment numbers when applicable. Any identification numbers associated with the suspect(s) other than those provided earlier are also beneficial, such as passport, alien registration, and driver's license numbers.

What instruments or mechanisms are being used to facilitate the suspect transaction(s)?

An illustrative list of instruments or mechanisms that may be used in suspicious activity includes, but is not limited to, wire transfers, letters of credit and other trade instruments, correspondent accounts, casinos, structuring, shell companies, bonds/notes, stocks, mutual funds, insurance policies, travelers checks, bank drafts, money orders, credit/debit cards, stored value cards, and/or digital currency business services. Specific suspect identifying information is provided in the relevant Suspicious Activity Report for RMLO filings.

In addition, a number of different methods may be employed for initiating the negotiation of funds such as the Internet, phone access, mail, night deposit box, remote dial-up, couriers, or others. In summarizing the flow of funds, always include the source of the funds (origination) that lead to the application for, or recipient use of, the funds (as beneficiary).

In documenting the movement of funds, identify all account numbers at the financial institution affected by the suspicious activity and when possible, provide any account numbers held at other institutions and the names/locations of the other financial institutions, including MSBs and foreign institutions involved in the reported activity.

When did the suspicious activity take place?

If the activity takes place over a period of time, indicate the date when the suspicious activity was first noticed and describe the duration of the activity. Filers will often provide a tabular presentation of the suspicious account activities (transactions in and out). While this information is useful and should be retained, do not insert objects, tables, or pre-formatted spreadsheets when filing a SAR. These items may not convert properly when keyed in or merged into the SAR System. Also, in order to better track the flow of funds, individual dates and amounts of transactions should be included in the narrative rather than just the aggregated amount.

Where did the suspicious activity take place?

Use the Narrative Section to indicate that multiple offices of a single financial institution were involved in the suspicious activity and provide the addresses of those locations. Specify if the suspected activity or transaction(s) involve a foreign jurisdiction. If so, provide the name of the foreign jurisdiction, financial institution, address and any account numbers involved in, or affiliated with the suspected activity or transaction(s).

Why does the filer think the activity is suspicious?

FinCEN suggests that the Company first describe briefly its industry or business – depository institution, casino, mortgage broker, mortgage banker, securities broker, insurance, real estate, investment services, money remitter, check casher, and so forth. Then describe, as fully as possible, why the activity or transaction is unusual for the customer: consider the types of products and services offered by the industry, and the nature and normally expected activities of similar customers.

Examples of some common patterns of suspicious activity are:

- a lack of evidence of legitimate business activity, or any business operations at all, undertaken by many of the parties to the transaction(s);
- unusual financial nexuses and transactions occurring among certain business types (e.g., food importer dealing with an auto parts exporter);
- transactions that are not commensurate with the stated business type and/or that are unusual and unexpected in comparison with the volumes of similar businesses operating in the same locale;
- unusually large numbers and/or volumes of wire transfers and/or repetitive wire transfer patterns;
- unusually complex series of transactions indicative of layering activity involving multiple accounts, banks, parties, jurisdictions;
- suspected shell entities;
- bulk cash and monetary instrument transactions;
- unusual mixed deposits of money orders, third party checks, payroll checks, etc., into a business account;
- transactions being conducted in bursts of activities within a short period of time, especially in previously dormant accounts;
- transactions and/or volumes of aggregate activity inconsistent with the expected purpose of the account and expected levels and types of account activity conveyed to the financial institution by the accountholder at the time of the account opening;
- beneficiaries maintaining accounts at foreign banks that have been subjects of previous SAR filings;
- parties and businesses that do not meet the standards of routinely initiated due diligence and anti-money laundering oversight programs (e.g., unregistered/unlicensed businesses);
- transactions seemingly designed to, or attempting to avoid reporting and recordkeeping requirements; and,
- accounts being utilized as “pass-through” points by foreign jurisdictions with subsequent outgoing funds to another foreign jurisdiction.

How did the suspicious activity occur?

Use the Narrative Section to describe the “modus operandi” or the method of operation of the subject conducting the suspicious activity. In a concise, accurate and logical manner, describe how the suspect transaction or pattern of transactions was committed. Provide as completely as possible a full picture of the suspicious activity involved. For example, if what appears to be structuring of currency deposits is matched with outgoing wire transfers from the accounts, the SAR narrative should include information about both the structuring and outbound transfers (including dates, destinations, amounts, accounts, frequency, and beneficiaries of the funds transfers).

APPENDIX R: ORGANIZING THE SAR NARRATIVE

When all applicable information is gathered, analyzed, and documented and the financial institution decides that a SAR is required, the information should be described in the SAR Narrative in a concise and chronological format. Include all elements of the five W's (**Who? What? When? Where? and Why?**) previously discussed (see Appendix Q) of this policy statement, as well as any other information that can assist law enforcement.

FinCEN suggests that the Company divide the narrative into three sections:

1. Introduction

2. Body

3. Conclusion

Introduction

The introductory paragraph can provide:

- the purpose of the SAR and a general description of the known or alleged violation [In some instances, this might warrant mentioning at the outset the type of suspicious activity being observed (i.e., smurfing, shell entities, complex layering activities, structuring, check kiting, embezzlement, and so forth];

- the date of any SAR(s) filed previously on the suspect or related suspects and the reason why the previous SAR(s) was filed;

- whether the SAR is associated with the Office of Foreign Assets Control's (OFAC) sanctioned countries or Specially Designated Nationals and Blocked Persons or other government lists for individuals or organizations;

- any internal investigative numbers used by the financial institution which may be a point of reference for law enforcement should the investigators wish to contact the institution; and

- a summary of the "red flags" and suspicious patterns of activity that initiated the SAR. (This information should be provided either in the introduction or conclusion of the narrative.)

Body

The next paragraph or paragraphs of the narrative can provide all pertinent information − supporting why the SAR was filed and might include:

- any and all relevant facts about the parties (individuals and businesses) who facilitated the suspicious activity or transactions. Include any unusual observations such as suspected shell entities; financial activities which are not commensurate with the expected normal business flows and types of transactions; unusual multiple party relationships; customer verbal statements; unusual and/or complex series of transactions indicative of layering; lack of business justification and documentation supporting the activity; and so forth;

- a specific description of the involved accounts and transactions, identifying if known, both the origination and application of funds (usually identified in chronological order by date and amount);

- breaking out larger volumes of financial activity into categories of credits and debits, and by date and amount;

- transactor and beneficiary information, providing as much detail as possible, including the name and location of any involved domestic and/or international financial institution(s); names, addresses, account numbers, and any other available identifiers of originator and beneficiary transactor(s) and/or third parties or business entities on whose behalf the conductor was acting; the date(s) of the transaction(s); and amount(s);

- an explanation of any observed relationships among the transactors (e.g., shared accounts, addresses, employment, known or suspected business relationships and/or frequency of transactions occurring amongst them; appearing together at the institution and/or counter);

- specific details on cash transactions that identify the branch(es) where the transaction(s) occurred, the type of transaction(s), and how the transaction(s) occurred (e.g., night deposit, on-line banking, ATM, etc.); and

- any factual observations or incriminating statements made by the suspect.

Conclusion

The final paragraph of the narrative can summarize the report and might also include:

- information about any follow-up actions conducted by the financial institution (e.g., intent to close or closure of accounts, ongoing monitoring of activity, and so forth);

- names and telephone numbers of other contacts at the financial institution if different from the point of contact indicated in the SAR;

- a general description of any additional information related to the reported activity that may be made available to law enforcement by the institution; and

- names of any law enforcement personnel investigating the complaint who are not already identified in another section of the SAR.

Important Reminder

Please do not include any supporting documentation with the Company's filed report nor use the terms "see attached" in the Narrative Section. When SAR forms are received at the IRS Detroit Computing Center (DCC), or such other facility that is designated to take physical receipt of a SAR, only information that is in an explicit, narrative format is keypunched. Thus, tables, spreadsheets or other attachments are not entered into the SAR System database.

Keep any supporting documentation in the Company's records for a period of five (5) years.

Law enforcement will contact the Company at the appropriate time to review any additional information.

APPENDIX S: CUSTOMER DUE DILIGENCE

As reflected in FinCEN guidance and enforcement actions, the cornerstone of a strong BSA/AML compliance program is the adoption and implementation of internal controls, which include comprehensive Customer Due Diligence ("CDD") policies, procedures, and processes for all customers, particularly those that present a high risk for money laundering or terrorist financing.

As part of their basic business model, financial institutions seek at some level to identify their customers and their needs in order to best service them. The requirement that a financial institution know its customers, and the risks presented by its customers, is basic and fundamental to the development and implementation of an effective BSA/AML compliance program.

In particular, appropriate CDD policies, procedures, and processes assist a financial institution in identifying, detecting, and evaluating unusual or suspicious activity.

Furthermore, financial institutions may not be able to perform effective risk assessments of their customers or account bases without conducting adequate due diligence throughout customer relationships.

SFI has an effective CDD program, providing information to develop a customer risk profile that can then be used by SFI to identify higher-risk customers and accounts, including customers and accounts subject to special or enhanced due diligence requirements.

SFI applies appropriate internal controls to identify and investigate unusual and suspicious activity and make an informed decision whether or not to file a SAR. In the event that the Company files a SAR, CDD information collected may enhance the information included in the SAR and thereby enhance law enforcement's ability to initiate and pursue the successful investigation and prosecution of criminal activity.

The failure to obtain adequate CDD information may impede SFI's ability to detect and report suspicious or unusual activity or provide information in a filing that is useful to law enforcement. Several of the consent orders and enforcement actions issued over the last few years have identified the lack of effective CDD policies, procedures, and processes, or the underlying elements thereof, as rendering AML programs inadequate, being a significant deficiency, and an underlying factor in supervisory actions.

Broadly, FinCEN believes that an effective CDD program includes the following elements:

1. Conducting initial due diligence on customers, which includes identifying the customer, and verifying that customer's identity as appropriate on a risk basis, at the time of account opening.

2. Understanding the purpose and intended nature of the account, and expected activity associated with the account for the purpose of assessing risk and identifying and reporting suspicious activity.

3. Except as otherwise provided, identifying the **beneficial owner(s)** of all customers, and verifying the beneficial owner(s)' identity pursuant to a risk-based approach. FinCEN currently defines "beneficial owner" is "an individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account".

4. Conducting ongoing monitoring of the customer relationship and conducting additional CDD as appropriate, based on such monitoring and scrutiny, for the purposes of identifying and reporting suspicious activity.

In order to implement the CDD procedures, the Company considers the following information:

A. Identification and Verification of the Customer

B. Understanding the Nature and Purpose of the Account

C. Obtaining Beneficial Ownership Information

D. Conducting Ongoing CDD

SFI's policies, procedures, and processes should include CDD guidelines that:

- Are commensurate with the Company's risk profile, paying particular attention to higher-risk customers.

- Contain a clear statement of management's overall expectations and establish specific staff responsibilities, including who is responsible for reviewing or approving changes to a customer's risk rating or profile, as applicable.

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

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

- Ensure the Company maintains current customer information.

Much of the CDD information may be confirmed through an information-reporting agency, banking references (for larger accounts), correspondence and telephone conversations with the customer, loan application information, and visits to the customer's house for a face-to-face application, or place of business. Additional steps may include obtaining third-party references or researching public information (e.g., on the Internet or commercial databases).

CDD processes include periodic risk-based monitoring of the customer relationship to determine whether there are substantive changes to the original CDD information (e.g., change in employment or business operations).

APPENDIX T: TIMING OF A SAR FILING

The SAR rules require that a SAR be filed 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 can be identified, the time period for filing a SAR is extended to 60 days.

The Company may need to review customer transaction or account activity to determine whether to file a SAR. The need for a review of customer activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the Company, 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 phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an accountholder's normal account activity. For example, a real estate investment (purchase or sale), the receipt of an inheritance, or a gift, may cause an account to have a significant credit or debit that would be inconsistent with typical account 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.
Whenever possible, an expeditious review of the transaction or the account is recommended and can be of significant assistance to law enforcement. In any event, the review should be completed in a **reasonable period of time**.

What constitutes a "reasonable period of time" will vary according to the facts and circumstances of the particular matter being reviewed and the effectiveness of the SAR monitoring, reporting, and decision-making process. The key factor is that the Company has established adequate procedures for reviewing and assessing facts and circumstances identified as potentially suspicious, and that those procedures are documented and followed in accordance with the SAR regulation and this policy statement.

For situations requiring immediate attention, in addition to filing a timely SAR, the Company will immediately notify, by telephone, an "appropriate law enforcement authority" and, as necessary, the Company's primary regulator or state banking department.

For this initial notification, an "appropriate law enforcement authority" would generally be the local office of the IRS Criminal Investigation Division or the FBI. Notifying law enforcement of a suspicious activity does not relieve a bank of its obligation to file a SAR.

For suspicious activity related to terrorist activity, the Company may also call FinCEN's Financial Institution's Terrorist Hotline at the toll-free number 866-556-3974 (7 days a week, 24 hours a day) to further facilitate the immediate transmittal of relevant information to the appropriate authorities.

APPENDIX U: SAR AUDIT – SCOPE AND TESTING

Objective: The Company uses the services of an independent external auditor to review its policies, procedures, and processes, and test the overall compliance with statutory and regulatory requirements for monitoring, detecting, and reporting suspicious activities.

The following outline includes, but is not limited to, certain aspects of the audit scope and testing implementation.

IDENTIFICATION OF UNUSUAL ACTIVITY

1. Review policies, procedures, and processes for identifying, researching, and reporting suspicious activity. Determine whether they include the following:

- 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, or National Security Letters (NSL)) for suspicious activity. NSLs are highly confidential documents; as such, auditors will not review or sample specific NSLs. Instead, auditors should evaluate the policies, procedures, and processes for:
  - o Responding to NSLs.
  - o Evaluating the account of the target for suspicious activity.
  - o Filing SARs, if necessary.
  - o Handling account closures.

2. Review the monitoring systems and how they fit into the Company's overall suspicious activity monitoring and reporting process

Transaction (Manual Transaction) Monitoring

3. Determine whether the transaction monitoring systems use reasonable filtering criteria whose programming has been independently verified. Determine whether the monitoring systems generate accurate reports at a reasonable frequency.

Surveillance (Automated Account) Monitoring

4. Identify the types of customers, products, and services that are included within the surveillance monitoring system.

5. Identify the system's methodology for establishing and applying expected activity or profile filtering criteria and for generating monitoring reports. Determine whether the system's filtering criteria are reasonable.

6. Determine whether the programming of the methodology has been independently validated.

7. Determine that controls ensure limited access to the monitoring system and sufficient oversight of assumption changes.

MANAGING ALERTS

8. Determine whether the Company has policies, procedures, and processes to ensure the timely generation of, review of, and response to reports used to identify unusual activities.

9. Determine whether policies, procedures, and processes require appropriate research when monitoring reports identify unusual activity.

10. Evaluate the policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. The process should ensure that all applicable information (e.g., criminal subpoenas, NSLs, and section 314(a) requests) is effectively evaluated.

11. Verify that staffing levels are sufficient to review reports and alerts and investigate items, and that staff possess the requisite experience level and proper investigatory tools. The volume of system alerts and investigations should not be tailored solely to meet existing staffing levels.

12. Determine whether the Company's SAR decision process appropriately considers all available Customer Due Diligence and Enhanced Due Diligence information.

SAR DECISION MAKING

13. Determine whether policies, procedures, and processes include procedures for:

- Documenting decisions not to file a SAR.
- Escalating issues identified as the result of repeat SAR filings on accounts.
- Considering closing accounts as a result of continuous suspicious activity.

SAR COMPLETION AND FILING

14. Determine whether 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.
- Sharing SARs with head offices and controlling companies, as necessary.

TRANSACTION TESTING

Transaction testing of suspicious activity monitoring systems and reporting processes is intended to determine whether the policies, procedures, and processes are adequate and effectively implemented.

The Company shall retain an independent auditor to document the factors used to select samples and should maintain a list of the accounts sampled. The size and the sample will be based on the following:

- Weaknesses in the account monitoring systems.
- The overall BSA/AML risk profile (i.e., number and type of higher-risk products, services, customers, entities, and geographies).
- Quality and extent of review by audit or independent parties.
- Prior examination and audit findings.
- Recent mergers, acquisitions, or other significant organizational changes.
- Conclusions or questions from the review of the SARs.

15. On the basis of a risk assessment, prior examination and audit reports, and a review of the audit findings, sample specific customer accounts to review the following:

- Suspicious activity monitoring reports.
- CTR download information, if applicable.
- Higher-risk banking operations (products, services, customers, entities, and geographies).
- Customer activity.
- Subpoenas received by the Company.
- Decisions not to file a SAR.

16. For the customers selected previously, obtain the following information, if applicable:

- CIP and account-opening documentation.
- CDD documentation.
- Two to three months of account statements covering the total customer relationship and showing all transactions.
- Sample items posted against the account (i.e., copies of checks deposited and written, debit or credit tickets, and funds transfer beneficiaries and originators).
- Other relevant information, such as loan files and correspondence.

17. Review the selected accounts for unusual activity. If the auditor identifies unusual activity, review customer information for indications that the activity is typical for the customer (i.e., the sort of activity in which the customer is normally expected to engage). When reviewing for unusual activity, consider the following:

- For individual customers, whether the activity is consistent with CDD information (e.g., occupation, expected account activity, and sources of funds and wealth).
- For business customers, whether the activity is consistent with CDD information (i.e., type of business, size, location, and target market).

18. Determine whether the transaction or surveillance suspicious activity monitoring system detected the activity that the auditor identified as unusual.

19. For transactions identified as unusual, discuss the transactions with management. Determine whether the BSA Officer demonstrates knowledge of the customer and the unusual transactions. After auditing the available facts, determine whether management knows of a reasonable explanation for the transactions.

20. Determine whether the Company has failed to identify any reportable suspicious activity.

21. From the results of the sample, determine whether the transaction or surveillance suspicious activity monitoring system effectively detects 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).

22. On the basis of a risk assessment, prior examination and audit reports, and a review of the audit findings, select a sample of management's research decisions to determine the following:

- Whether management decisions to file or not file a SAR are supported and reasonable.
- Whether documentation is adequate.
- Whether the decision process is completed and SARs are filed in a timely manner.

23. On the basis of a risk assessment, prior examination and audit reports, and a review of the audit findings, sample the SARs downloaded from the BSA reporting database or the internal SAR records. 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.
- If SAR narratives from the BSA reporting database are blank or contain language, such as "see attached," ensure that the Company is not mailing attachments to the IRS Enterprise Computing Center — Detroit (formerly the Detroit Computing Center).

[The IRS Enterprise Computing Center — Detroit's toll-free number is 800-800-2877.]

24. On the basis of audit procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with monitoring, detecting, and reporting suspicious activity.