sifma

Internal Auditors Society

Internal Audit Guidelines

Leading Practices in Auditing Anti-Money Laundering Programs

November 2017

The Audit Guidelines (the "guidelines") are intended to provide members of the Internal Auditors Society ("IAS"), a society of the Securities Industry and Financial Markets Association ("SIFMA"), with information for the purpose of developing or improving their approach towards auditing certain functions or products typically conducted by a registered broker-dealer. These guidelines do not represent a comprehensive list of all work steps or procedures that can be followed during the course of an audit and do not purport to be the official position or approach of any one group or organization, including SIFMA, or any of its affiliates or societies. Neither SIFMA, nor any of its societies or affiliates, assumes any liability for errors or omissions resulting from the execution of any work steps within these guidelines or any other procedures derived from the reader's interpretation of such guidelines. In using these guidelines, member firms should consider the nature and context of their business and related risks to their organization and tailor the work steps accordingly. Internal auditors should always utilize professional judgment in determining appropriate work steps when executing an audit. Nothing in these guidelines is intended to be legal, accounting, or other professional advice.

I. Introduction

Money laundering is defined as the process by which illegally obtained money appears to come from a legal or legitimate source. Money laundering involves three stages:

(1) Placement – Initial introduction of "dirty money" into the financial system;
(2) Layering – Distancing the money from its criminal or illegal source; and
(3) Integration – Distributing proceeds back to the illegal activity to make the money appear legitimate.

The Bank Secrecy Act ("BSA" or the "Act"), passed in 1970, began the modern era of promoting anti-money laundering ("AML") regulation in the United States. The BSA requires financial institutions to monitor and report suspicious activities and transactions, file currency transaction reports, and meet related record-keeping requirements. AML regulation escalated significantly after the September 11, 2001 terrorist attacks with the passage of the USA PATRIOT Act ("PATRIOT Act"), which imposed additional AML requirements on financial institutions. In particular, the PATRIOT Act mandates that financial institutions establish comprehensive AML compliance programs that help combat terrorist financing and money laundering activities. Covered financial institutions under the BSA include, but are not limited to, banks, broker-dealers, money services businesses, insurance companies, and registered investment companies.

The U.S. Department of Treasury's ("Treasury") Financial Crimes Enforcement Network ("FinCEN") has primary authority to implement, administer, and enforce compliance with the BSA and associated regulations. FinCEN has issued various rules for financial institutions, including information sharing pursuant to Section 314(a) and customer due diligence requirements. In addition to BSA and PATRIOT Act requirements, the Financial Industry Regulatory Authority (FINRA) has provided the most comprehensive set of regulatory guidelines for broker-dealers. Specifically, Rule 3310[1] requires that member firms develop and implement a written AML program reasonably designed to achieve and monitor the member's compliance with the requirements of the BSA, and the implementing regulations promulgated thereunder by the Department of the Treasury. Financial institutions, including broker-dealers, have received fines and other sanctions for AML program failures in recent years.

While the leading practices and suggested test steps outlined within these guidelines are targeted for broker-dealers, those member firms that are subsidiaries of banks or bank holding companies should further consider bank-specific federal and/or state imposed AML requirements and guidance, including those outlined by the Federal Financial Institutions Examination Council (FFIEC)[2] and the New York State Department of Financial Services (DFS)[3]. In general, state requirements should be evaluated for applicability depending on the registration status of each financial institution.

Outside the U.S., AML regulations have grown in importance as well. The Financial Conduct Authority in the UK, the Ontario Securities Commission, other provincial Canadian regulators, and the Monetary Authority of Singapore have also issued AML regulations for financial institutions.

[1] FINRA: Notice to Members 09-60: http://www.finra.org/sites/default/files/NoticeDocument/p120229.pdf "FINRA, SEC Approves Consolidated FINRA Rules, October 2009, FINRA Rule 3310"
[2] FFIEC: https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf, "Federal Financial Institutions Examination Council, Bank Secrecy Act/ Anti-Money Laundering Examination Manual"
[3] New York State DFS: http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp504t.pdf, "Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications"

II. Key Risks and Considerations

In preparing for the audit, the auditor should (1) develop a working knowledge of applicable requirements under the Act, (2) meet with relevant business "first line of defense" and compliance "second line of defense" counterparts within the firm, (3) assess the overall culture of compliance, and (4) determine if there were material changes to the firm's business (including new services or products offerings) and control environment (including AML system implementations, enhancements, or conversions) that may impact the relative money-laundering risk.

The following topics and risks should be considered during the review:

1. AML Program

- **a. Internal Policies, Procedures, and Controls –** A firm should maintain current, complete and clear policies and procedures outlining the controls in place to mitigate the firm's AML risks**.**
- **b. Compliance Officer –** The AML Compliance Officer has the full responsibility for implementing and monitoring the day-to-day operations and internal controls of the firm's Anti-Money Laundering compliance program. The duties of the AML Compliance Officer will include monitoring the firm's compliance with AML obligations, ensuring independent audits, and employee training. The Compliance Officer must be reported to FINRA.
- **c. Training –** Poorly trained personnel may compromise the effectiveness of the AML program.
- **d. Independent Test –** To comply with requirements of the Act and FINRA and MSRB rules, member firms must ensure an annual review is conducted by a qualified and independent party. FINRA does allow for an "every other year review" in certain circumstances based on factors outlined in FINRA Rule 3310. Due to FINRA's "calendar year" requirement, member firms must ensure the review is conducted and completed accordingly.
- **e. Customer Due Diligence – *NEW* –** On May 11, 2016, FinCEN published a final rule that formalizes new and existing Customer Due Diligence (CDD) requirements for broker-dealers in securities, mutual funds, futures commission merchants and introducing brokers in commodities. Covered financial institutions must comply with the Final Rule by May 11, 2018. The rule describes four core elements of CDD that are required for the AML programs of covered financial institutions: (1) identifying and verifying the identity of customers, subject to certain exceptions, (2) identifying and verifying the identity of beneficial owners and control persons of legal entity customers, subject to certain exceptions, (3) understanding the nature and purpose of customer relationships to develop a customer risk rating, or profile, and (4) ongoing monitoring for reporting suspicious transactions and, on a risk basis, maintaining and updating beneficial owner information. In advance of the applicability date, auditors should consider assessing the adequacy of the firm's response through review of technical specifications, timelines, and progress against milestones.

2. Customer Identification Program

A firm's Customer Identification Program (CIP) must include risk-based procedures for verifying the identity of each customer, subject to certain exceptions, to the extent reasonable and practicable. The procedures must be based on the firm's assessment of the relevant risks, including those presented by the various types of accounts maintained by the broker-dealer, the various methods of opening accounts, the various types of identifying information available, and the broker-dealer's size, geographic location(s) and customer base.

3. Suspicious Activity Identification and Reporting

There are a wide range of criteria (or "red flags") that may indicate potentially suspicious activity resulting from money laundering or terrorist financing, all coming from a wide array of sources. The range of products and services offered by the firm along with the firm's client base are essential in order to understand the potential sources of suspicious activity and to evaluate if the proper controls and surveillance to detect and report such activity are in place.

4. **Special Measures**

   The U.S. Treasury Department periodically designates financial institutions, foreign jurisdictions, transactions, or account types as a "primary money laundering concern." This designation can result in up to five different special measures being imposed. Firms are notified by the U.S Treasury Department of additions/removals and firms should develop procedures for complying with the restrictions imposed by an active "special measure," including prohibiting establishment of accounts or transactions, if applicable.

5. **Foreign Correspondent Account Due Diligence**

   Broker-dealers are prohibited from establishing, maintaining, administering or managing correspondent accounts for, or on behalf of, foreign "shell" banks and generally must perform risk-based due diligence of foreign correspondent accounts. To the extent applicable, the Act requires that firms perform additional due diligence for specific sets of accounts including: correspondent accounts owned by foreign financial institutions (including enhanced due diligence and information collection for correspondent accounts owned by foreign banks) and foreign private banking accounts.

6. **Information Sharing**

   Firms are (1) required to respond to FinCEN requests for account/transaction information and (2) on a voluntary basis, able to register for and receive safe harbor when sharing information with other financial institutions in an attempt to gather information related to potential suspicious activity.

7. **Currency Transaction Reporting**

   Financial institutions must report large currency transactions via a Currency Transaction Report (CTR) for individual or aggregate transactions greater than or equal to $10,000 USD. The definition of "transaction" includes deposits, withdrawals, exchanges, or payments/transfers of currency. Certain transactions meeting specific criteria are exempt from this reporting requirement.

8. **Travel Rule Requirements and Recordkeeping**

   Per the BSA, broker-dealers involved in a transmittal of funds are required to obtain and retain specific information associated with the funds transmitted when greater than or equal to $3,000. The information that must be collected depends on the institution's role in the transmittal of funds (i.e., Transmittor, Intermediary, or Recipient). The information collected also depends on whether the transmittor or recipient is an established customer of the broker-dealer and/or whether the transmittal was done in person.

Refer to the *Appendix* herein for suggested test steps, guidelines, and additional considerations for the above and other related topics.

Regulatory References:

FINRA: Guidance: http://www.finra.org/industry/what-expect-anti-money-laundering-reviews-during-routine-examinations, "What to Expect: Anti-Money Laundering Reviews During Routine Examinations"

FinCEN: https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions, "Federal Register, Customer Due Diligence Requirements for Financial Institutions, A Rule by the Financial Crimes Enforcement Network, May 11, 2016"

FinCEN: https://www.fincen.gov/answers-frequently-asked-bank-secrecy-act-bsa-questions, "Answers to Frequently Asked Bank Secrecy Act (BSA) Questions"

SEC: https://www.sec.gov/about/offices/ocie/amlsourcetool.htm, "Anti-Money Laundering Source Tool for Broker-Dealers, January 11, 2017" *(includes links to enforcement actions)*

1. AML Program Components

a. Internal Policies, Procedures and Controls

The auditor should obtain the firm's AML policies and procedures and perform the following:

- Confirm the procedures are up-to-date and comprehensive (e.g., address current regulatory requirements; include considerations for all relevant lines of business).
- Verify control activities include responsible parties, frequency, method, segregation of duties, approval, etc.
- Evaluate documentation accessibility for relevant personnel.
- Verify approval from appropriate levels of senior management following material changes, to the extent required by the firm's policies and procedures.

b. Compliance Officer

The auditor should confirm member firms have formally appointed and approved the AML Compliance Officer and submitted the following required information to FINRA:

- Name of the AML Compliance Person;
- Full organizational title;
- Mailing address and email address;
- Telephone and fax number;
- Emergency contact information; and
- Changes within 30 days and an annual verification by mid-January each year.

The auditor should also confirm that the AML Compliance Officer reviews and addresses heightened due diligence and "red flag" issues that are relevant to the line(s) of business. In addition, the auditor should evaluate the following as it relates to the office and activities of the AML Compliance Officer:

- Approvals and regulatory filings are timely and complete.
- The experience, authority, and independence of the AML Compliance Officer appear adequate. For example, the auditor may confirm that the AML Compliance Officer is a primary advisor to the firm on the compliance program and demonstrates independence from colleagues, clients and the board. In addition, the auditor should confirm that the AML Compliance Officer demonstrates (1) competence and is knowledgeable regarding how the particular business is managed based on its risk of money laundering and (2) knowledge regarding enforcement actions, regulatory authority, and relevant regulatory risks to the firm.
- Any Board and Senior Executive management reporting, to the extent required by the firm's policies and procedures, is thorough and presented at appropriate intervals.
- Key staff is competent, participates in relevant training initiatives, understands and utilizes mechanisms to escalate concerns, and has appropriate access to report potential red flag issues to the AML Compliance Officer.

c. Training

The auditor should evaluate the firm's ongoing anti-money laundering training program to evaluate the completeness, accuracy, and applicability of training content, including:

- Overview of regulations and requirements (federal, state, international) and the firm's policies and procedures to comply;
- Customized firm-specific risks and/or applicability;

- Relevant red flags and signs of money laundering;
- Escalation protocols; and
- Consequences of non-compliance.

The auditor should also evaluate the availability and completeness of training records, including audience selection criteria, basis for excluded personnel, and rationale for non-completion records, and may wish to further consider the following:

- Training frequency, method/medium (online, in person, outsourcing, use of native language), and opportunities for automation, where appropriate;
- Interactive nature (case studies, knowledge test questions, etc.);
- Requirements and timing for new employee onboarding training;
- Role-specific supplemental training for higher-risk personnel (customer-facing, AML Compliance, alert reviewers, SAR filers); and
- Executive management/Board-specific training in addition to sponsorship and support (tone at the top).

d. Independent Test

To comply with requirements of the Act and FINRA and MSRB rules, member firms must ensure an annual review is conducted by a qualified and independent party. FINRA does allow for an every other year review in certain circumstances based on factors outlined in FINRA Rule 3310. Due to FINRA's "calendar year" requirement, member firms must ensure the review is conducted and completed accordingly.

e. Customer Due Diligence - *NEW*

Covered financial institutions must comply with FinCEN's Final Rule by May 11, 2018. The rule describes four core elements of CDD that are required for the AML programs of covered financial institutions:

- Identifying and verifying the identity of customers, where applicable;
- Identifying and verifying the identity of beneficial owners of legal entity customers, subject to certain exceptions;
- Understanding the nature and purpose of customer relationships to develop a customer risk profile; and
- Ongoing monitoring for reporting suspicious transactions and, on a risk basis, maintaining and updating customer information.

The first element is covered under existing CIP rules, and the second element is a new requirement. FinCEN states that the third and fourth elements are already implicit in the suspicious activity reporting requirements but have been explicitly added as the "fifth pillar" of an effective AML program.

The Final Rule's definition of "beneficial owner" consists of two "prongs":

- Under the ownership prong, a beneficial owner is each individual (if any) who, directly or indirectly, owns 25 percent or more of the equity interests of a legal entity customer. This prong would require identification of no more than four individuals and, if no individual meets the 25 percent threshold, no individuals would need to be identified.
- Under the control prong, a beneficial owner is a single individual with significant responsibility to control, manage or direct a legal entity customer, including (i) an executive officer or senior

manager (e.g., CEO, CFO, COO, Managing Member, General Partner, President, Vice President or Treasurer) or (ii) any other individual who regularly performs similar functions.

Given that the effective date for compliance is in 2018, the auditor should assess the firm's readiness efforts to comply with the new rule, including reasonableness of implementation timelines, information technology updates, training, etc. Upon the compliance effective date, CDD-related audit procedures should be determined while planning the annual CIP testing.

2. Customer Identification Program

The auditor should review CIP procedures to confirm there are provisions for the following:

- Obtaining identifying information from each customer prior to account opening;
- Verifying the identity of each customer, either through documentary or non-documentary methods, within a reasonable time before or after account opening;
- Making and maintaining a record of information obtained relating to identity verification (i.e., name, street address, SSN or TIN, and date of birth for individuals);
- Determining within a reasonable time after account opening or earlier whether a customer is a foreign or domestic politically exposed person or appears on any list of known or suspected terrorist organizations designated by Treasury[4]; and
- Providing each customer with adequate notice, prior to opening an account, that information is being requested to verify the customer's identity.

The auditor should perform testing to confirm CIP controls are designed effectively and operating as designed. This can be achieved in a variety of ways including, but not limited to, the following:

- For a sample of new accounts, confirm that the required customer information was provided by the client timely (prior to account funding) and is accessible.
- For a sample of new accounts verified via a third-party service provider (e.g., Equifax), confirm that customers who could not be verified are restricted from account activity and appropriate action was taken timely by the firm for all customers that could not be verified.
- Confirm that CIP system logic considers/includes all relevant account and relationship types and assess any account type exclusions for reasonableness.
- Evaluate activities performed by the 'second line of defense' such as quality assurance reviews performed by AML compliance and confirm the reviews identify and remediate CIP-related exceptions or overrides.
- Obtain the CIP notice language and delivery methods and evaluate for reasonableness.

The auditor should also determine if there is a CIP delegation agreement in place. The CIP rule provides that, under certain defined circumstances, a firm may rely on the performance of another financial institution to fulfill some or all of the requirements of the broker-dealer's CIP. For example, in order for a firm to rely on another financial institution, the other financial institution also must be subject to an AML compliance program rule and be regulated by a federal functional regulator. If such an agreement(s) exists, the auditor should obtain and review the contract between the broker-dealer and other financial institution, in addition to the annual certification from the financial institution stating, amongst other things, that the financial institution will perform the specified requirements of the firm's CIP.

[4] At the time of publication of these guidelines, there are no designated government lists of known or suspected terrorists or terrorist organizations to verify customers specifically for CIP. The Office of Foreign Assets Control lists and FinCEN Section 314(a) government lists remain separate and distinct requirements.

The use of third-party vendors to perform CIP activities should also be evaluated by the auditor. Audit procedures should include evaluating the controls and review procedures the firm executes to confirm the vendor is adhering to the requirements set forth in the contract, as it relates to CIP. As with any vendor relationship, data security, privacy, feed completeness, and data integrity controls should also be considered by the auditor.

3. Suspicious Activity Identification and Reporting

As a baseline, the auditor should be familiar with the range of products and services offered by the firm, along with an understanding of the firm's client base, in order to understand the potential sources of suspicious activity and to evaluate if proper controls to detect and report such activity are in place.

Broker-dealers have an obligation to file[5] Suspicious Activity Reports ("SARs") with FinCEN for:

- Transactions conducted or attempted by, at, or through the broker-dealer and aggregating funds or other assets of at least $5,000, if the broker-dealer knows, suspects, or has reason to suspect that the transaction:
  - Involves funds derived from illegal activity or is intended to disguise funds derived from illegal activity;
  - Is designed, whether through structuring or other means, to evade the BSA or its implementing regulations; or
  - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

The auditor should consider the following methods for evaluating the design and operating effectiveness of the control activities within the firm intended to (1) prevent or detect potentially suspicious activity and (2) file timely and accurate reports with FinCEN:

- Verify that automated surveillance system source data, including customer and transactional data, negative media, etc., comes from appropriate sources and systems (this may require the assistance of integrated information technology audit specialists) and is accurate and complete.
- Test automated surveillance system filtering criteria, also sometimes known as scenarios or models, to verify that (1) the purpose is documented and deemed reasonable in light of the risk, and (2) they are subject to controls to prevent inappropriate modification.
- Validate that automated surveillance is working as designed (i.e., periodic model validation).
- Confirm there are processes and controls to adjust the settings within automated surveillance systems to allow for an appropriate level of false positives.
- Test that alerts from the automated transaction surveillance systems are investigated timely and contain adequate documentation to either clearly and sufficiently dispose of the alert or validate the decision to investigate further in order to file a SAR.
- Review organizational charts and résumés to determine whether staffing is adequate from both a headcount and qualification perspective to ensure that the volume of alerts can be sufficiently managed.

[5] 31 CFR 1023.320 outlines the specific requirements for broker-dealers in securities to file with FinCEN a report of any suspicious transaction indicating a possible violation of law or regulation.

- Review aging of alerts to identify any backlogs.
- Confirm that other sources of potentially suspicious activity (e.g., manual referrals from other lines of businesses within the firm, 314(a) requests, etc.) are treated in a similar fashion to automated alerts and tracked similarly.
- Review management information reports to ensure that all alerts (both automated and referrals) are identified, are sufficiently granular (e.g., location, type of activity, aging, etc.), and are provided to senior management, as required by the firm's policies and procedures.
- Assess the policies and procedures specific to potential SAR investigations, including alert and referral intake procedures, standard research elements, escalation protocols, cycle times, etc.
- Review a sample of cases with a non-filing determination, including the underlying documentation supporting the decision for reasonableness, confirming that the supporting materials provide adequate rationale for a qualified third party to understand.
- For a sample of filed SARs, confirm the form is accurately and completely populated, the narrative includes appropriate detail, and the rationale for filing the SAR is reasonable (i.e., not simply defensive).
- Assess quality assurance reviews performed for completeness, timeliness, and adequate follow-up actions.
- Test timeliness of the electronic SAR filing process to verify the forms are filed within 30 days of initial detection of facts that may constitute the filing of a SAR.
- Verify that senior management is informed of SAR filings on a routine basis, as appropriate.
- Verify that safeguards exist to prevent potential "tipping-off" of a SAR filing to the clients in question.

4. Special Measures

The auditor should review the firm's procedures for prohibiting establishment of accounts or transactions with the entities/jurisdictions with an active "special measure[6]." Audit procedures may include reviewing records of the existing customer base to determine if appropriate prohibitions are in place where needed and that potential matches have been escalated.

5. Foreign Correspondent Account Due Diligence

The auditor should ensure the firm has policies and procedures in place that prohibit establishing, maintaining, administering or managing correspondent accounts for, or on behalf of, foreign "shell" banks and establish risk-based due diligence procedures for foreign correspondent accounts. To the extent applicable, the auditor should perform the following procedures to evaluate the relevant controls:

- Review the protocols for identifying the accounts subject to this requirement (correspondent accounts owned by foreign financial institutions, including foreign banks, and foreign private banking accounts) for completeness.
- Confirm that the firm has collected and reviewed pertinent information on these accounts to evidence that risk-based due diligence (e.g., obtaining and reviewing the foreign financial institution's AML program, monitoring transactions, collecting and reviewing beneficial ownership information, identifying politically exposed foreign persons associated with the account) is performed at the time the account is established and on an ongoing basis.

[6] FinCEN Special Measures for Jurisdictions, Financial Institutions, or International Transactions of Primary Money Laundering Concern: https://www.fincen.gov/resources/statutes-and-regulations/311-special-measures

6. Information Sharing

The auditor should perform the following procedures (including sample testing where warranted) around the mandatory 314(a) and voluntary 314(b) information sharing:

- Confirm dedicated firm points of contact have been assigned, and FinCEN is notified timely of changes.
- Verify that responsible parties maintain records including; original request, searches performed and disposition of false positives, and evidence of successful submissions to FinCEN for 314(a) or communications to other financial institutions for 314(b).
- Evaluate 314(a) procedures to confirm search parameters match the request (i.e., time frame, names, etc.) and false positives have proper documentation.
- If applicable based on participation in voluntary information sharing, determine that the annual notifications to FinCEN for 314(b) participation are available and complete (though lack of notifications would not constitute a regulatory violation, as participation is voluntary).

7. Currency Transaction Reporting

The auditor should assess whether Currency Transaction Reporting (CTR) is applicable to the firm based on whether or not it deals in currencies. If applicable, the auditor should test the firm's processes to ensure regulatory requirements are being followed. Specifically, the auditor should:

- Review business line procedures and confirm there are processes for preparing, retaining and filing CTRs in a timely manner (15 days after transaction) unless the Line of Business specifically prohibits transactions in currency.
- Confirm that there are processes to review electronic notifications received from FinCEN's BSA E-Filing system and take corrective action when necessary (i.e., errors, warnings, rejections).
- Confirm there are procedures to identify and report on transactions that in aggregate meet reporting thresholds, and confirm the means for aggregation is appropriate (i.e., TIN, customer number).
- Confirm that personnel do not have the capability to override currency aggregation systems. If override capability exists, review the controls in place to ensure the capability is used appropriately. Controls may include supervisory approval, generation of exception reports, and AML Compliance Officer's review of exception reports.
- Confirm that there are procedures to escalate potential suspicious activity for customers attempting to evade the reporting threshold.
- Select a sample of reportable transactions, including those that individually meet the reporting requirement and for clients with aggregate amounts in a single day that meet the reporting requirement, and confirm that CTRs were completed in accordance with FinCEN instructions.

Currency Transaction Reporting Exemptions

The auditor should evaluate each business line to determine if an exemption applies and is being used. If so, the auditor should confirm the following:

- A "Designation of Exempt Person" report was appropriately completed and filed within 30 days of the first reportable transaction.
- The Person or Entity being exempted meets the requirements of Phase I or Phase II CTR exemptions and the reason for exemption is reasonable and documented.
- Customers with exemptions are reviewed at least annually to ensure they continue to meet the exemption eligibility requirements.

- There are procedures to monitor customers with exemptions for potentially suspicious activity.

8. Travel Rule Requirements and Recordkeeping

The auditor should perform transaction testing by obtaining a population of transmittals of funds greater than or equal to $3,000, while considering each of the different roles that the institution plays in the transfer (i.e., Transmittor, Intermediary, Recipient) and each of the relevant systems that process transmittals of funds. The test plan should include verifying each of the required criteria is retained and available for the population/period sampled. The auditor should consult the regulation and relevant publicly available FAQs to confirm the test procedures include each of the relevant data elements.

9. OFAC and Global Sanctions

The auditor should determine whether the AML audit scope will incorporate sanctions compliance objectives. The Department of the Treasury's Office of Foreign Assets Control[7] ("OFAC") administers economic sanctions against certain countries, individuals, companies and groups based on foreign policy or national security concerns. OFAC sanctions generally prohibit U.S. persons and companies from transacting directly or indirectly with sanctions targets and require that firms block transactions and freeze assets associated with the sanctions targets. While OFAC regulations are not part of the BSA, and OFAC itself does not require a formal sanctions compliance program or independent review, evaluation of OFAC compliance is frequently included in BSA/AML regulatory examinations. While not specific to the securities industry, regulatory expectations for the frequency of these reviews vary from annually to every 18-24 months depending on the type of institution and guidance issued by the applicable regulatory authorities.

If included in the audit scope, the auditor should assess the firm's OFAC and global sanctions compliance policies and procedures to evaluate whether they are comprehensive, accurate, aligned with regulatory requirements/expectations, and appropriate for the risk of non-compliance, taking into consideration the firm's products, services, customers, entities, transactions, geographic locations and use of third-party vendors.

OFAC and Global Sanctions Lists

The auditor should evaluate whether relevant sanctions lists[8] (including OFAC's Specially Designated Nationals, or SDN, list) are maintained internally or if a third-party service is used. In either instance, the auditor should assess the lists for accuracy and completeness. Audit tests may include independently verifying completeness of the lists using data analysis techniques and confirming the most recent updates are reflected within the sanctions lists used by the firm for any compliance screening processes.

Of particular interest to the securities industry, OFAC published the Sectoral Sanctions Identification (SSI) List[9] in 2014 through Directives issued under Executive Order 13662 identifying sanctions targets operating in specific sectors of the Russian economy. These Directives prohibit transactions in,

[7] OFAC: https://www.treasury.gov/resource-center/sanctions/Documents/facbk.pdf - Regulations for the Financial Community - Information about the laws and regulations OFAC administers.

[8] OFAC: Sanctions Lists: https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx

[9] OFAC: Ukraine/Russia-Related Sanctions Program: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/ukraine.pdf

financing for, and other dealings in new debt of longer than 30 or 90 days maturity and/or new equity associated with the named sanctions targets. The SSI list is not part of the SDN list, but individuals or companies on the SSI list may also appear on the SDN list.

Sanctions Screening – Transactions and Accounts

It is important to note that while screening accounts and transactions is not an explicit OFAC requirement, firms generally employ either internal or third-party vendor screening tools to achieve compliance with OFAC and other similar global regulations that prohibit transactions with sanctions targets.

The auditor should evaluate the firm's processes to monitor or screen transactions prior to acceptance or execution and perform timely verification of new and existing customer accounts against relevant sanctions lists. The auditor should determine the most appropriate testing method based on whether screening controls are automated or manual. If the control is systematic or automated, the auditor should confirm that system logic is designed to appropriately produce expected results (i.e., halt the transaction or restrict the account pending further review). If the control is manual, the auditor should evaluate whether screening was performed timely using current sanctions lists. Additionally, the auditor may select a sample of transaction and account records and verify that transactions were not executed and/or accounts were restricted until any screening alerts were resolved.

If systematic screening tools are leveraged, the auditor should:

- Assess the screening tool system logic and validate that the firm has clearly defined its criteria for comparing names on sanctions lists with the names on customer/transaction records.
- Determine if system logic is working as designed and effective by tracing a sample of records through the logical flow of the system.
- Determine whether the firm's screening system is reviewed periodically and considered for updates, based on factors including volume of false positive alerts.
- Validate that the screening criteria used by the firm to identify name and language variations and misspellings are based on the level of risk associated with the particular product or type of transaction and transaction volume.

Blocked / Rejected Transactions

The auditor should evaluate the adequacy of the processes and controls in place to block or reject non-compliant transactions as follows:

- Verify procedures reflect the operating environment and have been communicated to the appropriate stakeholders.
- Confirm that the escalation or communication processes related to preventing unauthorized release of funds exist and are operating effectively.
- For a sample of blocked accounts, determine if the account balance has changed since the account funds were frozen. If there was a change in account balance, determine the reason and whether escalation occurred based on the facts and circumstances.

OFAC Regulatory Reporting

For a sample of blocked/rejected transactions during the test period, the auditor should inspect the OFAC reporting documentation and confirm the following:

- Blocking/rejecting details are documented completely and accurately.

- The report was transmitted to OFAC within 10 days of the block/rejection and is/was included on the annual reporting to OFAC (note timing differences where appropriate).
- Information sent to OFAC includes all relevant details.
- Management review and oversight is documented related to blocking process.
- Records are retained as required.

10. Compliance Testing

FINRA Rule 3120 requires that for certain firms (i.e., ≥ $200M revenue) the annual certification process must include, amongst other things, a discussion of compliance efforts related to anti-money laundering. The auditor should determine whether the AML audit scope will include Rule 3120 compliance objectives and, if so, obtain and review evidence related to the discussion of AML compliance efforts and evaluate for reasonableness. In addition, to the extent that other groups within the firm (e.g., business line compliance, enterprise risk) have performed AML related control testing, the auditor should review the results and confirm that issues identified have been adequately addressed.

11. Information Technology

Throughout all applicable sections of the Act and corresponding audit scope areas, the auditor should consider and assess relevant information technology systems and controls supporting fundamental compliance with AML requirements, especially those supporting suspicious activity monitoring, SAR filing, 314(a) and Global Sanctions screening, and the customer identification processes. Particular areas of focus should include, but are not limited to:

- Data integrity and completeness (e.g., incomplete/inaccurate/corrupt data);
- Data source/feed completeness (e.g., headers and trailers, record counts, data security);
- Access management (e.g., inappropriate access, access provisioning);
- Change management (e.g., audit trail, documented approvals);
- System parameters/logic (e.g., exclusions, thresholds, criteria, timeframe); and
- Cybersecurity controls.

Additionally, in recent years, FINRA has highlighted examination results[10] that indicate weaknesses with firms' automated trading and money movement surveillance systems "not capturing complete and accurate data, which can result in missed or poor quality alerts" as well as "poorly set parameters or surveillance patterns that do not capture problematic behavior." The auditor should evaluate the adequacy of the firm's surveillance and screening systems specific to the firm's customer base and associated money laundering risks and also consider the frequency and results of related system testing, including testing associated with new system implementations, logic changes/enhancements, and quality assurance reviews.

12. AML Governance

Although embedded at nearly every step of the detailed testing listed above, the auditor should consider additional governance activities as part of an overall assessment of the AML program. While AML governance activities are not explicit requirements under the Act, and these activities may vary widely by firm, the auditor should consider these examples:

[10] 2016 and 2017 Annual Regulatory and Examination Priorities Letters: http://www.finra.org/industry/annual-regulatory-and-examination-priorities-letters

BSA/AML risk assessments: While not a requirement under the Act, the auditor should evaluate any BSA/AML risk assessments, if available, for completeness and accuracy of inherent risks, mitigating controls, and residual risks. If the firm has not performed BSA/AML risk assessments, the auditor should consider whether risk assessments may be warranted given the complexity of the firm's business (e.g., products and services, transactional volume, customer demographic, etc.) as well as applicable regulatory expectations.

Success measures: The auditor should evaluate how the AML Compliance Officer determines the success of the institution's AML program. Based on established measures, the auditor should consider reviewing the underlying data used for accuracy and methods used to improve the AML program when success measures are not being met.

Vendor management: Based on the third-party vendors engaged in AML program activities, the auditor should evaluate the initial selection and vetting of the vendor(s) as well as the ongoing evaluation of the effectiveness of the vendor(s) for reasonableness and compliance with relevant contract provisions (e.g., adhering to data integrity protocols, providing SSAE 16 reports, etc.).

Guidance: The auditor should review enterprise-wide guidance set forth by the AML Compliance Officer and evaluate whether it meets minimum standards for compliance and outlines the activities to be performed by the second line of defense (AML or business line compliance).