Hot Topics in AML
Wednesday, October 16, 2019
3:10 p.m. – 4:00 p.m.

Join regulatory staff and industry experts as they discuss changes impacting the anti-money laundering (AML) and financial crime environment. Panelists discuss new areas of focus and effective practices.

Moderator:
Joseph McNulty
Examination Manager, Sales Practice
FINRA Philadelphia District Office

Speakers:
Sarah Green
Global Head of Financial Crimes
Vanguard Group, Inc.

Eli Renshaw
Examination Manager
FINRA Anti-Money Laundering Investigative Unit (AMLIU)

Glenn Skreppen
Director, Bureau of Securities Compliance and Examinations
Pennsylvania Department of Banking and Securities

Hot Topics in AML Panelist Bios:

Moderator:

Joe McNulty is Examination Manager in FINRA's District 9A-Philadelphia office. He manages a team of six Examiners who are responsible for conducting firm examinations. His team has been associated with several high profile investigations that have identified serious sales practice abuses. Prior to becoming an Examination Manager, Mr. McNulty was an Examiner in FINRA's District 9B-Woodbridge office responsible for conducting examinations in FINRA's Cycle, Cause, and New Membership Application programs. Before joining FINRA, Mr. McNulty worked in the Compliance department of a wirehouse firm investigating customer complaints and disclosure matters.

Speakers:

Sarah D. Green is Global Head of Financial Crimes Officer for Vanguard Group, Inc. She joined Vanguard in December, 2017 and leads compliance teams responsible for Vanguard's anti-money laundering (AML), trade surveillance, anti-bribery and corruption and sanctions programs. She worked previously as the Senior Director for AML Compliance at FINRA, where she supervised FINRA's dedicated AML examination unit and coordinated FINRA's AML enforcement cases. Ms. Green was also responsible for FINRA AML guidance and external training of financial industry professionals domestically and internationally, and she represented FINRA on the Bank Secrecy Act Advisory Group. Previously, she was the Bank Secrecy Act Specialist in the Division of Enforcement's Office of Market Intelligence (OMI) at the U.S. Securities and Exchange Commission (SEC). In this role, she oversaw the Commission's review and use of suspicious activity reports (SARs) and worked with Enforcement staff on AML matters. Prior to joining OMI, Ms. Green was a branch chief in the Office of Compliance Inspections and Examination at the SEC, managing the Commission's AML examination program for broker-dealers, including developing examination modules, conducting training for SEC and self-regulatory organization (SRO) staff and coordinating with the SROs on all aspects of AML examination and enforcement. Prior to joining the SEC, Ms. Green was an associate attorney in the Corporate and Securities practice group at Gardner Carton & Douglas LLP. Ms. Green received her J.D. from the William and Mary School of Law and her B.A. from Hamilton College.

Eli Renshaw joined the (formerly known as) NASD in 1999 after completing his service as a US Army officer. During his career at FINRA, Mr. Renshaw has led major fraud and AML related examinations across the country. Mr. Renshaw currently works as an examination manager in FINRA's AML Investigative Unit and is a FINRA national subject matter expert on AML. Mr. Renshaw holds a BS in Finance from Drexel University and is CAMS certified.

Glenn Skreppen is Director of the Bureau of Securities Compliance and Examinations for the Pennsylvania Department of Banking and Securities. He manages securities investigations and investment adviser/broker-dealer compliance examinations for the Commonwealth of Pennsylvania. Previously, he worked for BNY Mellon as the Head of Domestic Equity Trading for their Securities Lending Department. He is a graduate of Indiana State University with a Bachelor's Degree in Accounting, and he earned an MBA in Finance from the University of Pittsburgh. Mr. Skreppen is a member of the NASAA Enforcement Training Project Group and the International Association of Financial Crimes Investigators (IAFCI). He holds the designations of Certified Fraud Examiner (CFE) and Certified Anti-Money Laundering Specialist (CAMS).

FINRA District Compliance Seminar

With the State of Pennsylvania

October 16, 2019 | Harrisburg, PA

Hot Topics in AML

Panelists

Moderator

- Joseph McNulty, Examination Manager, Sales Practice, FINRA Philadelphia District Office

Panelists

- Sarah Green, Global Head of Financial Crimes, Vanguard Group, Inc.
- Eli Renshaw, Examination Manager, FINRA Anti-Money Laundering Investigative Unit (AMLIU)
- Glenn Skreppen, Director, Bureau of Securities Compliance and Examinations, Pennsylvania Department of Banking and Securities

To Access Polling

- **Please get your devices out:**
  - **Type the polling address, https://finra.cnf.io/sessions/wqcc, into the browser**
  - **Select your polling answer**
    - **Note:** Each session will have a different polling address.

Polling Question 1

1. **Are the Bank Secrecy Act requirements, including filing a Suspicious Activity Report (SAR), applicable to digital assets regardless of whether such assets are securities?**
   a. **Yes**
   b. **No**

Polling link: https://finra.cnf.io/sessions/wqcc

Polling Question 2

2. For a broker-dealer's anti-money laundering program to be compliant with the applicable securities rules and regulations, it must incorporate and address all possible "red flags" that may be applicable to the securities industry?
   a. Yes
   b. No

Polling link: https://finra.cnf.io/sessions/wqcc

Hot Topics in AML

- **Notice-To-Members 02-21: NASD Provides Guidance To Member Firms Concerning Anti-Money Laundering Compliance Programs Required by Federal Law**
- **Regulatory Notice 19-18: FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations**

Hot Topics in AML

- **Regulatory Notice 19-18 – Categories of Potential Red Flags**
  - **Potential Red Flags in Customer Due Diligence and Interactions with Customers**
  - **Potential Red Flags in Deposits of Securities**
  - **Potential Red Flags in Securities Trading**
  - **Potential Red Flags in Money Movements**
  - **Potential Red Flags in Insurance Products**
  - **Other Potential Red Flags**

Hot Topics in AML

FinCEN's Customer Due Diligence Requirements for Financial Institutions and FINRA Rule 3310

- The four components of customer due diligence:
  - Customer Identification and Verification
  - Beneficial Ownership Identification and Verification
  - Understanding the Nature and Purpose of Customer Relationships
  - Ongoing Monitoring for Reporting Suspicious Transactions and Maintaining Customer Information

Hot Topics in AML

Areas of Concern

- Digital Assets
- Elder Financial Abuse
- Private Placements
- Regulatory Technology
- Outsourcing to Third Parties

Hot Topics in AML

Resources

- FINRA: ***www.finra.org***
- SEC: ***www.sec.gov***
- PA Department of Banking and Securities: ***www.dobs.pa.gov***
- Financial Action Task Force: ***www.fatf-gafi.org***

INFORMATIONAL

Anti-Money Laundering

NASD Provides Guidance To Member Firms Concerning Anti-Money Laundering Compliance Programs Required By Federal Law

SUGGESTED ROUTING

The Suggested Routing function is meant to aid the reader of this document. Each NASD member firm should consider the appropriate distribution in the context of its own organizational structure.

- Legal & Compliance
- Operations
- Registration
- Senior Management

KEY TOPICS

- Compliance Programs
- Money Laundering

Executive Summary

On October 26, 2001, President Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act).[1] Title III of the PATRIOT Act, referred to as the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (Money Laundering Abatement Act), imposes obligations on broker/dealers under new anti-money laundering (AML) provisions and amendments to the existing Bank Secrecy Act (BSA) requirements.[2]

Among other things, the Money Laundering Abatement Act requires all financial institutions, including broker/dealers, to establish and implement, by **April 24, 2002**, AML programs designed to achieve compliance with the BSA and the regulations promulgated thereunder. The NASD reminds members that violations of the AML laws could lead to criminal prosecution.

On February 15, 2002, the NASD filed with the Securities and Exchange Commission (SEC) a rule proposal to prescribe the minimum standards required for each member firm's AML compliance program. A copy of this rule filing can be found on the NASD Regulation AML Web Page. (*See www.nasdr.com/money.asp.*) NASD Regulation's AML Web Page also provides links to other sites and documents to assist members in understanding their obligations under the AML rules and regulations.

On February 25, 2002, the SEC published the proposed rule change in the *Federal Register*. The SEC received four comment letters in response to the *Federal Register* publication. Before becoming effective, the proposed rule change must be approved by the SEC.

The Securities Industry Association Anti-Money Laundering Committee recently released a preliminary guide for firms to use when developing their AML programs (SIA Guidance). The SIA Guidance generally discusses key elements for broker/dealers to consider in developing effective AML programs. NASD Regulation's AML Web Page provides a link to the SIA Guidance.

The NASD is issuing this *Notice* to provide guidance to assist members in developing AML compliance programs that fit their business models and needs. A table of contents has been provided for readers' convenience.

Because the Department of Treasury (Treasury) is still developing AML rules, the NASD will update its guidance as new rules become final. In the interim, firms must comply with the current requirements of the BSA and the provisions of the Money Laundering Abatement Act that now apply to broker/dealers and should familiarize themselves with the proposed rules that Treasury has issued to date. (For links to Treasury's proposed rules, *see www.nasdr.com/money.asp*.)

Questions/Further Information

Questions regarding this *Notice to Members* may be directed to Nancy Libin, Assistant General Counsel, Office of General Counsel, NASD Regulation, at (202) 728-8835; Grace Yeh, Assistant General Counsel, at (202) 728-6939; or Kyra Armstrong, Senior Attorney, Department of Member Regulation, at (202) 728-6962.

Anti-Money Laundering Notice to Members

TABLE OF CONTENTS

BACKGROUND

The PATRIOT Act is designed to detect, deter, and punish terrorists in the United States and abroad and to enhance law enforcement investigation tools by prescribing, among other things, new surveillance procedures, new immigration laws, as well as new and more stringent AML laws. The Money Laundering Abatement Act expands and strengthens the AML provisions put into place by earlier legislation.

Several provisions of the Money Laundering Abatement Act are relevant to NASD members. Among other things, all broker/dealers must implement an anti-money laundering compliance program by April 24, 2002. The Money Laundering Abatement Act also requires Treasury to promulgate rules requiring broker/dealers to file suspicious activity reports (SARs), which identify and describe transactions that raise suspicions of illegal activity, and to establish certain procedures with regard to "correspondent accounts" maintained for foreign banks.[3] In late December 2001, Treasury released proposed rules regarding the filing of SARs by broker/dealers[4] and the maintenance of "correspondent accounts" for foreign banks.[5] In late February 2002, Treasury released proposed and final rules governing information sharing among law enforcement authorities, regulatory organizations, and financial institutions.[6] Treasury will continue to issue proposed and final rules throughout the year governing and providing further guidance with respect to customer identification, "correspondent accounts" with foreign banks, and the application of AML rules to the brokerage industry, among other matters. The NASD will continue to keep members apprised of AML rules and regulations that Treasury proposes and those that Treasury adopts.

INTRODUCTION

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering occurs in connection with a wide variety of crimes, including, but not limited to, drug trafficking, robbery, fraud, racketeering, and terrorism.

In general, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash profits from criminal activity are converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to separate further the proceeds from their criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund further criminal or legitimate activities.[7]

Broker/Dealers And Existing Anti-Money Laundering Laws

Broker/dealers are subject to most of the existing AML rules as well as the new AML provisions of the Money Laundering Abatement Act, which are discussed in detail later in the document.

Firms should be aware that there are potential severe civil and criminal penalties for violations of AML laws. Under the criminal statutes, a person or entity could be criminally prosecuted for assisting or facilitating a transaction involving money laundering by a customer if the firm (or person) knew or was willfully blind to the fact that the transaction involved illegally obtained funds.[8]

All broker/dealers have been and will continue to be subject to existing BSA reporting and recordkeeping requirements, as briefly summarized below:

- **Currency Transaction Report (CTR):** Broker/dealers are required to file CTRs for transactions involving currency that exceed $10,000. Because structuring is prohibited, multiple transactions are treated as a single transaction if they total more than $10,000 during any one business day. CTRs are filed with the Financial Crimes Enforcement Network (FinCEN), a bureau of Treasury.
- **Currency and Monetary Instrument Transportation Report (CMIR):** Any person who physically transports, mails, or ships currency or other monetary instruments into or out of the United States, in aggregated amounts exceeding $10,000 at one time, must report the event on a CMIR. Any person who receives any transport, mail, or shipment of currency, or other monetary instrument from outside the United States in an aggregate amount exceeding $10,000 at one time also must report the receipt. CMIRs are filed with the Commissioner of Customs.
- **Report of Foreign Bank and Financial Accounts (FBAR):** Any person having a financial interest in, or signature or other authority over, financial accounts in a foreign country is required to report the relationship if the aggregate value of the accounts exceeds $10,000. FBARs are filed with FinCEN.
- **Funds Transfers and Transmittals:** Broker/dealers effecting transmittals or transfers of funds, including wire fund transfers, of $3,000 or more must collect, retain and record on the transmittal order certain information regarding the transfer, including the name and address of the transmitter and recipient, the amount of the transmittal order, the identity of the recipient's financial institution, and the account number of the recipient. Broker/dealers also must verify the identity of transmitters and recipients that are not established customers.

In addition, broker/dealers that are subsidiaries of banks or bank holding companies currently are required under the banking regulations to file SARs with FinCEN. Such broker/dealers currently are required to report known or suspected federal criminal offenses, at specified dollar thresholds, or suspicious transactions involving $5,000 or more that they suspect (1) involve funds derived from illegal activity or an attempt to hide or disguise funds or assets derived from illegal activity, (2) are designed to evade the requirements of the BSA, or (3) have no apparent lawful or business purpose or vary substantially from normal practice. The NASD previously has recommended that members report suspicious transactions and has advised firms that the failure to do so could be construed as aiding and abetting money laundering violations, subjecting the member to civil and criminal liability.[9] Some firms, in fact, have been submitting SARs on a voluntary basis. As discussed in more detail later in the document, all broker/dealers will soon be required to file SARs.

New And Expanded Anti-Money Laundering Laws Applicable To Broker/Dealers

As noted above, the Money Laundering Abatement Act imposes significant new obligations on broker/dealers through new AML provisions and amendments to the existing provisions of the BSA. A brief summary of the new requirements along with anticipated effective dates is provided below:

- **Section 312 (Due Diligence Requirements):** Section 312 requires special due diligence for all private banking and "correspondent" bank accounts (accounts established to receive deposits from, make payments on behalf of, or handle other financial transactions for a foreign bank) involving foreign persons, even if opened before Congress passed the PATRIOT Act.[10] Treasury is required to delineate, by regulation, the special due diligence

policies, procedures, and controls by April 24, 2002. Regardless of whether final regulations have been promulgated, the minimum due diligence requirements set forth in Section 312 (as discussed below in the "Anti-Money Laundering Program Guidance" section) become ***effective on July 23, 2002***.

- **Section 313 (Correspondent Account Prohibitions):** Section 313 prohibits certain financial institutions, including broker/dealers, from maintaining a "correspondent account" for, or on behalf of, a foreign "shell" bank (a foreign bank with no physical presence in any country). Financial institutions are also required to take reasonable steps to ensure that they are not indirectly providing correspondent banking services to foreign shell banks through foreign banks with which they maintain correspondent relationships. Section 313 became ***effective on December 26, 2001***. Treasury released proposed regulations defining "correspondent account" in late December 2001.[11]

- **Section 314 (Financial Institution Cooperation Provisions):** Section 314 addresses increased cooperation among financial institutions, regulatory authorities, and law enforcement authorities. Treasury published regulations implementing Section 314 in the *Federal Register* on March 4, 2002.[12] Treasury included a proposed rule to establish a communication link between federal law enforcement and financial institutions to better share information relating to suspected terrorists and money launderers. In addition, Treasury issued an interim final rule, ***effective March 4, 2002***, requiring financial institutions to file an initial, and annual thereafter, certification (which can be completed online at FinCEN's Web Site at *www.treas.gov/fincen*) if they wish to share information regarding terrorist financing and money laundering with other financial institutions or associations of financial institutions.[13]

- **Section 319(b) (Domestic and Foreign Bank Records Production):** Section 319(b) addresses the production of domestic and foreign bank records. A financial institution is required to produce account information relating to foreign bank accounts **within seven days** in response to requests from federal law enforcement. Section 319 became **effective on *December 26, 2001***. As mentioned above, Treasury released proposed rules regarding maintaining "correspondent accounts" in late December 2001.[14]

- **Section 326 (Customer Identification Standards):** Section 326 requires Treasury and the SEC, jointly, to issue regulations that set forth minimum standards for customer identification in the account opening process. The regulations will need to require firms, at a minimum, to implement "reasonable procedures" to verify the identity of the customer opening an account, maintain records used to identify the customer, and consult government-provided lists of known or suspected terrorists. Final regulations prescribed under Section 326 will take effect **not later than *October 26, 2002***. Treasury and the SEC have not yet released proposed regulations regarding customer identification.

- **Section 352 (AML Compliance Program Components):** Section 352 requires all financial institutions to develop and implement AML compliance programs **on or before *April 24, 2002***. Section 352 requires the compliance programs, at a minimum, to establish (1) the development of internal policies, procedures, and controls, (2) the designation of a compliance officer with responsibility for a firm's anti-money laundering program, (3) an ongoing employee training program, and (4) an independent audit function to test the effectiveness of the anti-money laundering compliance program. Section 352 further requires Treasury by April 24, 2002, to issue regulations that consider the extent to which these requirements correspond to the size, location, and activities of different financial institutions. Section 352 further allows Treasury, at its discretion, to issue additional requirements for AML compliance programs before the April 24, 2002, deadline. As further discussed later in the document, the NASD has proposed a rule setting forth the minimum standards for its members' AML compliance programs.

- **Section 356 (Broker/Dealer SAR Regulations): By *July 1, 2002***, Treasury must publish final regulations requiring broker/dealers to file SARs. Treasury released proposed broker/dealer SAR regulations in late December 2001.[15] Under Treasury's proposed regulations, the suspicious activity reporting requirement would become effective *180 days after the date on which the final broker/dealer SAR regulations are published in the Federal Register*.

NASD ANTI-MONEY LAUNDERING PROGRAM RULE

On February 15, 2002, the NASD filed with the SEC a rule proposal that would set forth minimum standards for broker/dealers' AML compliance programs.[16] As required by the Money Laundering Abatement Act itself, the rule proposal would require firms to develop and implement a written AML compliance program by April 24, 2002. The proposed rule would require the program to be approved in writing by a member of senior management and be reasonably designed to achieve and monitor the member's ongoing compliance with the requirements of the BSA and the implementing regulations promulgated thereunder. The proposed rule change would require firms, at a minimum, to:

(1) establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of suspicious transactions;

(2) establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the BSA and implementing regulations;

(3) provide for independent testing for compliance to be conducted by member personnel or by a qualified outside party;

(4) designate an individual or individuals responsible for implementing and monitoring the day-to-day operations and internal controls of the program; and

(5) provide ongoing training for appropriate personnel.

Each firm's AML program must be designed to ensure compliance with the new provisions of the Money Laundering Abatement Act, the earlier provisions of the BSA, and the regulations promulgated thereunder. To be effective, those procedures must reflect the firm's business model and customer base. Further, in developing program criteria, firms should consider the guidelines established by the United States Sentencing Commission in the U.S. Sentencing Commission Guidelines for organizations, as well as the fiduciary responsibilities of officers and directors to ensure that the firm's compliance programs are viable and effective.[17]

Regardless of when and in what form the SEC approves the NASD proposed AML compliance rule, all firms are required by federal law (the Money Laundering Abatement Act) to have AML programs in place **by April 24, 2002**.[18] These AML programs must meet the minimum requirements articulated in Section 352 of the Money Laundering Abatement Act.[19]

Members should keep in mind that the obligation to develop and implement an AML compliance program is not a "one-size-fits-all" requirement. The general nature of the requirement reflects Congressional intent that each financial institution should have the flexibility to tailor its AML program to fit its business. This flexibility is designed to ensure that all entities covered by the statute, from the very large financial institutions to the small firms, will institute effective and appropriate policies and procedures to monitor for AML compliance.[20] In this regard, each broker/dealer, in developing an appropriate AML program that complies with the Money Laundering Abatement Act, should consider factors such as its size, location, business activities, the types of accounts it maintains, and the types of transactions in which its customers engage.

ANTI-MONEY LAUNDERING PROGRAM GUIDANCE

The required elements of an AML program are discussed in detail below.

Develop Internal Policies, Procedures, And Controls

Broker/dealers must develop internal policies, procedures, and controls to ensure compliance with the AML laws. The AML procedures should contain a statement that sets forth the member's policy of prohibiting money laundering and its overall efforts to detect, deter, and prevent any such violations. Broker/dealers also must establish internal controls to ensure that their AML policies and procedures are being enforced. As with any supervisory procedure, the firm must establish and implement controls and written procedures that explain the procedures that must be followed, the person responsible for carrying out such procedures, how frequently such procedures must be performed, and how compliance with the procedures should be documented and tested.

Firms must determine the manner in which AML procedures that address the following (each of which will be discussed more fully below) will apply to various accounts:

- account opening and maintenance, including verification of the identity of the customer;
- opening and maintaining "correspondent accounts" for foreign banks;
- monitoring of account activities, including but not limited to, trading and the flow of money into and out of the account, the types, amount, and frequency of different financial instruments deposited into and withdrawn from the account, and the origin of such deposits and the destination of withdrawals;
- separating the duties of employees where feasible to ensure a system of checks and balances (for example, firms may want to ensure that persons who handle cash do not open accounts or file CTRs);
- monitoring for, detecting, and responding to "red flags";
- responding to regulatory requests for AML information;
- establishing controls and monitoring employees' trading and financial activity in employee accounts; and
- ensuring that AML compliance programs contain a mechanism or process for the firm's employees to report suspected violations of the firm's AML compliance program procedures and policies to management, confidentially, and without fear of retaliation.

Identification And Verification Of Account Holders

Opening Accounts

Prior to the enactment of the Money Laundering Abatement Act, broker/dealers already had significant obligations to gather information about their customers in order to, among other things, know their customers. NASD Rule 3110 requires member firms to obtain certain information about their customers when opening an account, including the following: the customer's name and residence; whether the customer is of legal age; the signature of the registered representative introducing the account and signature of the member or partner, officer, or manager who accepts the account; and if the customer is a corporation, partnership, or other

legal entity, the names of any persons authorized to transact business on behalf of the entity. Member firms are also required to make reasonable efforts to obtain the following additional information (for accounts other than institutional accounts and accounts in which investments are limited to transactions in open-end investment company shares not recommended by the member or its associated persons) prior to the settlement of an initial transaction in the account: a customer's tax identification and Social Security number; the customer's occupation and name and address of the employer; and whether the customer is an associated person of another member.

Member firms also are required under NASD Rules 2110 and 2310 to obtain additional customer information. Members are required under NASD Rule 2110 to comply with general "Know Your Customer" requirements. Pursuant to these requirements, members must make reasonable efforts to obtain certain basic financial information from customers so that members can protect themselves and the integrity of the securities markets from customers who do not have the financial means to pay for transactions.[21] NASD Rule 2310 relates to a member's suitability obligations to its customers and requires each member to use reasonable efforts to obtain information concerning a customer's financial status, tax status, and investment objectives prior to making any recommendations to the customer regarding the purchase, sale, or exchange of securities.

The information required under NASD Rules 3110, 2110, and 2310 is the starting point for new AML customer identification procedures. The Money Laundering Abatement Act imposes additional customer identification requirements on member firms. Effective October 26, 2002 (or earlier, if final customer identification regulations are effective prior to October 26, 2002), broker/dealers are required to implement reasonable procedures for identifying customers and verifying their information.[22] These procedures, at a minimum, must require a firm:

- to verify, to the extent reasonable and practicable, the identity of any customer seeking to open an account;[23]
- to maintain records of information to verify a customer's identity; and
- to check that a customer does not appear on any list of known or suspected terrorists or terrorist organizations such as those persons and organizations listed on Treasury's Office of Foreign Assets Control (OFAC) Web Site (*www.treas.gov/ofac*) (and available on *www.nasdr.com/money.asp*) under "Terrorists" or "Specially Designated Nationals and Blocked Persons" (SDN List), as well as the list of embargoed countries and regions (collectively, the OFAC List).[24]

Under the new AML customer identification requirements, broker/dealers will be required to make reasonable efforts to obtain and verify information about a customer. If the customer is an individual, a firm will need, to the extent reasonable and practicable, to obtain and verify certain information concerning the individual's identity, such as the individual's name, address, date of birth, and government issued identification number. Possible sources of this information include:

- physical documents, such as a driver's license, passport, government identification, or an alien registration card,[25] or, for businesses, a certificate of incorporation, a business license, any partnership agreements, any corporate resolutions, or other similar documents; or
- databases, such as Equifax, Experion, Lexis/Nexis, or other in-house or custom databases.

Firms opening accounts should verify the identification information at the time the account is opened, or within a relatively short time period thereafter (*e.g.*, within five business days after account opening). Because of the unknown risk that the prospective customer could be involved

in criminal activity, members should consider, depending on the nature of a transaction and an account, not effecting a transaction prior to verifying the information. If a potential customer refuses to provide any of the information described above, or appears to have intentionally provided false or misleading information, a firm should not open the account. If an existing customer fails to provide the requested information, the firm, after considering the known and unknown risks involved, may consider closing the account. Moreover, in either of these situations, the firm's AML compliance personnel should be notified so that a determination can be made as to whether the circumstance should be voluntarily reported to FinCEN or OFAC, as appropriate.

In the context of AML compliance, members should implement procedures that allow the firm to collect and use information concerning the account holder's wealth, net worth, and sources of income to detect and deter possible money laundering activity. Such a review should be integrated into the new accounts supervisor's existing procedures before such supervisor authorizes the opening of an account. Moreover, the supervisor's review should be documented and reviewed to ensure that the account-opening procedures are being conducted properly. Firms should consider using a checklist that lists the types of information required and documents explanations for why an account was opened absent such information.

Online Brokers

Online brokers generally do not meet or speak directly to their prospective or existing clients. These firms must acquire information about customers and, as mentioned earlier, make maximum use of other means of verifying customer identity, such as electronic databases (Equifax, Experion, Lexis/Nexis, or other in-house or custom databases). As is required of all firms, such verification of customer information must take place at the time the account is opened or within a short period thereafter (*e.g.*, five business days). Online firms should also consider conducting computerized surveillance of account activity to detect suspicious transactions and activity. Given the global nature of online brokerage activity, it is essential that online brokers confirm the customer data and review the OFAC List to ensure that customers are not prohibited persons or entities and are not from embargoed countries or regions.

Additional Due Diligence When Opening An Account

Broker/dealers should perform the following additional due diligence when opening an account, depending on the nature of the account, and to the extent reasonable and practicable:

- inquire about the source of the customer's assets and income so that the firm can determine if the inflow and outflow of money and securities is consistent with the customer's financial status;
- gain an understanding of what the customer's likely trading patterns will be, so that any deviations from the patterns can be detected later on, if they occur;
- maintain records that identify the owners of accounts and their respective citizenship;
- require customers to provide street addresses to open an account, and not simply post office addresses, or "mail drop" addresses;
- periodically contact businesses to verify the accuracy of addresses, the place of business, the telephone, and other identifying information; and
- conduct credit history and criminal background checks through available vendor databases.

Prohibitions On U.S. Correspondent Accounts With Foreign Shell Banks And Special Due Diligence For Correspondent Accounts

Broker/dealers are prohibited from establishing, maintaining, administering, or managing a "correspondent account" (*see* note 3) in the United States for an unregulated foreign shell bank. Firms should have procedures in place to ensure that this does not occur and should immediately terminate such accounts if they have any. The broker/dealer's AML compliance personnel should be notified upon discovery or suspicion that the firm may be maintaining or establishing a "correspondent account" in the United States for a foreign shell bank.

The Money Laundering Abatement Act requires broker/dealers to maintain records identifying the owners of foreign banks that maintain "correspondent accounts" in the United States and the name and address of an agent residing in the United States authorized to accept service of legal process for such banks.[26] Broker/dealers should require their foreign bank account holders to complete model certifications issued by Treasury to the extent possible. U.S. depository institutions and broker/dealers can send the certification forms to their foreign bank account holders for completion. The certification forms generally ask the foreign banks to confirm that they are not shell banks and to provide the necessary ownership and agent information. Use of the certification forms will help firms ensure that they are complying with requirements concerning "correspondent accounts" with foreign banks and can provide a broker/dealer with a safe harbor for purposes of complying with such requirements.[27] Firms are required to recertify (if relying on the certification forms) or otherwise verify any information provided by each foreign bank, or otherwise relied upon, at least every two years or at any time the firm has reason to believe that the information is no longer accurate.

In addition, broker/dealers will be required under Section 312 of the Money Laundering Abatement Act to establish appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering for any "correspondent account" established, maintained, administered, or managed for a foreign bank. *At a minimum*, in the case of foreign banks licensed by certain high-risk jurisdictions or operating under an offshore banking license, broker/dealers are required to take reasonable steps:

- to determine the ownership of the foreign bank;
- to conduct enhanced scrutiny of the account to detect and report suspicious activity; and
- to determine whether the foreign bank maintains "correspondent accounts" for any other bank, and if so, the identity of those banks.[28]

Special Due Diligence For Private Banking Accounts

Similarly, the Money Laundering Abatement Act requires broker/dealers, *at a minimum*, to take reasonable steps to determine the identity of the nominal and beneficial account holders of, and the source of funds deposited into, a private banking account maintained by or on behalf of a non-U.S. citizen, and to conduct enhanced scrutiny of accounts requested or maintained by, or on behalf of, a senior foreign political figure,[29] or any immediate family member or close associate of a senior foreign political figure. A private bank account is an account (or combination of accounts) that requires an aggregate deposit of funds or other assets of more than $1,000,000 established on behalf of one or more individuals who have a direct or beneficial ownership interest in the account, and is assigned to, or administered by, in whole or in part, an officer,

employee, or agent of a financial institution acting as a liaison between the institution and the direct or beneficial owner of the account.[30] This enhanced monitoring or scrutiny should be reasonably designed to detect and report transactions that may involve the proceeds of foreign official corruption.[31] Broker/dealers should monitor future pronouncements from Treasury, while also determining the extent to which they offer "private banking accounts," and ensure that their AML compliance program includes enhanced monitoring and scrutiny of accounts requested or held on behalf of foreign officials who may be involved in corrupt activities. The special due diligence requirements discussed in this section will become effective on July 23, 2002, regardless of whether Treasury has promulgated final regulations.

Monitoring Accounts For Suspicious Activity

The Money Laundering Abatement Act requires Treasury to adopt regulations requiring broker/dealers to file SARs.[32] Under Treasury's proposed regulations, SARs would be filed with FinCEN. Broker/dealers would be required to file SARs for:

- any transaction conducted or attempted by, at or through a broker/dealer involving (separately or in the aggregate) funds or assets of $5,000 or more for which:
    - the broker/dealer detects any known or suspected federal criminal violation involving the broker/dealer, or
    - the broker/dealer knows, suspects, or has reason to suspect that the transaction:
        - involves funds related to illegal activity,[33]
        - is designed to evade the regulations, or
        - has no business or apparent lawful purpose 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.

Although the reporting threshold begins at $5,000, in its proposed regulations, Treasury notes that a risk-based approach to developing compliance procedures that can be reasonably expected to promote the detection and reporting of suspicious activity should be the focus of a broker/dealer's AML compliance program. Treasury further notes that a compliance program that allows for the review of only those transactions that are above a set threshold, regardless of whether transactions at a lower dollar threshold may involve money laundering or other risks, would probably not be a satisfactory program.[34] Broker/dealers should file a SAR and in some circumstances notify law enforcement authorities of all transactions that arouse articulable suspicion that proceeds of criminal, terrorist, or corrupt activities may be involved.

Treasury could amend its proposed regulations based on comments it receives from interested parties. Treasury is required to issue final SAR regulations by July 1, 2002, and firms will be required to file SARs beginning 180 days after final broker/dealer SAR regulations are published in the *Federal Register*. To demonstrate a strong commitment to compliance with AML principles and goals, broker/dealers should consider filing SARs voluntarily prior to the effective date of the regulations. NASD Regulation will keep members informed as Treasury's proposed regulations are amended and finalized.

Money Laundering "Red Flags"

Broker/dealers need to look for signs of suspicious activity that suggest money laundering.[35] If a broker/dealer detects "red flags," it should perform additional due diligence before proceeding with the transaction. Examples of "red flags" are described below:

- The customer exhibits unusual concern regarding the firm's compliance with government reporting requirements and the firm's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force (FATF).[36]
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer's account shows numerous currency or cashiers check transactions aggregating to significant sums.
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.

- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other "red flags," engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" (Reg S) stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent business purpose or other purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.[37]

The above-listed money laundering "red flags" are not exhaustive; however, an awareness of the "red flags" will help ensure that broker/dealer personnel can identify circumstances warranting further due diligence. Appropriate "red flags" should be described in the written policies and AML compliance procedures of the broker/dealer.

Reporting Procedures

Although final regulations concerning the filing of SARs may not be adopted until July 1, 2002, voluntary reporting is useful to the government and helpful to firms in order to provide a defense to charges of aiding and abetting money laundering violations. Furthermore, in anticipation of the adoption of the final broker/dealer SAR requirements, all broker/dealers should be preparing to establish and implement procedures to detect and report suspicious transactions by means of SARs. Firms should implement systems, preferably automated ones, that would allow firms to monitor trading, wire transfers, and other account activity to allow firms to determine when suspicious activity is occurring. If a firm decides to monitor customer accounts manually, it must review a sufficient amount of account activity to ensure the detection of suspicious activity by allowing the member to identify patterns of activity and more importantly, new patterns or patterns that are inconsistent with the customer's financial status or make no economic sense.

Exception reports should consider the transaction size, location, type, number, and the nature of the activity. Firms should create guidelines for employees that identify examples of suspicious activity that may involve money laundering and form lists of high-risk clients whose activities may warrant further scrutiny. Firms should develop procedures for following-up on transactions that have been identified as suspicious or high-risk.

Broker/dealers should also develop administrative procedures concerning SARs. The procedures should address the process for filing SARs and reviewing SAR filings and the frequency of filings for continuous suspicious activity. In addition, a broker/dealer should consider requiring that all of its SAR filings be reported periodically to its Board of Directors and/or to senior management. In the event of a high-risk situation, broker/dealers should require that a report be made immediately to the Board of Directors and/or senior management.[38]

Recordkeeping And Disclosure

Firms should develop procedures to maintain the confidentiality of the SAR filings and to maintain copies of SARs for a five-year period. Firms are prohibited from notifying any person involved in a reported transaction that the transaction has been reported on a SAR. In addition, firms may not disclose SARs or the fact that a SAR was filed, other than to law enforcement agencies or securities regulators. Firms must also have procedures in place to ensure the denial of any subpoena requests for SARs or information in SARs, and for informing FinCEN of any subpoena received. It may be advisable to segregate SAR filings and supporting documentation from other books and records of the firm to avoid violating the prohibitions on disclosure of these records. The broker/dealer should also establish procedures and identify a contact person to handle requests for a subpoena or other requests that call for disclosure of a SAR.

Currency Transaction Reports

Broker/dealers should have procedures to ensure compliance with the BSA provision requiring broker/dealers to file CTRs with FinCEN.

Currency And Monetary Instrument Transportation Reports

Broker/dealers should have procedures to ensure compliance with the BSA provision requiring broker/dealers to file CMIRs with the Commissioner of Customs when any person physically transports, receives, mails, or ships currency or other monetary instruments into or out of the United States, in aggregated amounts exceeding $10,000 at one time.

Procedures For Sharing Information With And Responding To Requests For Information From Federal Law Enforcement Agencies

Broker/dealers should develop procedures to handle requests for information from FinCEN relating to money laundering or terrorist activity. Under Treasury's *proposed* regulations implementing Section 314, which were published in the *Federal Register* on March 4, 2002, FinCEN may require broker/dealers to search their records to determine whether they maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. If a broker/dealer identifies an account or transaction identified by FinCEN, it would be required to report the identity of the individual, entity, or organization, the account number, all identifying information provided by the account holder when the account was established, and the date and type of transaction. Broker/dealers would be required to report the information to FinCEN as soon as possible either by e-mail to *patriot@fincen.treas.gov*, by calling the Financial Institutions Hotline (1-866-556-3974), or by any other means that FinCEN specifies.

Broker/dealers also should identify contact persons and have procedures in place for providing information to and handling requests from enforcement authorities about the firms' AML efforts, as well as customers engaged in possible money laundering. This information must be provided to the appropriate agency and made available at a specified location when requested. Firms should establish procedures to provide such information *not later than seven days* after receiving a written enforcement agency request.

Firms should also have procedures in place to terminate a correspondent relationship with a foreign bank *within 10 business days* of receiving written notice from Treasury or the United States Attorney General that the foreign bank failed either to comply with a summons or subpoena or to contest it in United States court.

Finally, in the course of performing due diligence or during the opening of an account, firms should immediately contact Federal law enforcement by telephone in appropriate emergency situations as described below:

- a customer is listed on the OFAC List;
- a customer's legal or beneficial account owner is listed on the OFAC List;
- a customer attempts to use bribery, coercion, undue influence, or other inappropriate means to induce a broker/dealer to open an account or proceed with a suspicious or unlawful activity or transaction; and
- any other situation that a firm reasonably determines requires immediate government intervention.

Voluntary Information Sharing Among Financial Institutions

To the extent desired and/or appropriate, broker/dealers should have procedures in place for sharing information with other financial institutions about those suspected of terrorism and money laundering. Under Treasury's *interim rule*, which became effective on March 4, 2002, broker/dealers that share this information must file an annual certification with FinCEN.[39] The certification requires broker/dealers to take steps necessary to protect the confidentiality of the information and to use the information only for purposes specified in the rule. The certification can be found at: *www.treas.gov/fincen*. Broker/dealers should have adequate procedures to protect the security and confidentiality of such information.

Designate Compliance Officer

Every broker/dealer compliance program must designate a compliance officer ("AML Compliance Officer") to help administer the firm's AML compliance program efforts. Broker/dealers should vest this person with full responsibility and authority to make and enforce the firm's policies and procedures related to money laundering. The AML Compliance Officer does not need to be the firm's current compliance officer. Some larger firms have placed this responsibility on the firm's risk manager. Firms may, however, consider incorporating AML compliance requirements into the existing duties of a firm compliance officer. Whomever the firm designates as its AML Compliance Officer should have the authority, knowledge, and training to carry out the duties and responsibilities of his or her position.

The AML Compliance Officer should monitor compliance with the firm's AML program and help to develop communication and training tools for employees. The AML Compliance Officer should also regularly assist in helping to resolve or address heightened due diligence and "red flag" issues.

The AML Compliance Officer should ensure that AML records are maintained properly and that SARs are filed as required pursuant to the firm's procedures. In short, the AML Compliance Officer should be the primary contact for the firm on AML compliance implementation and oversight.

Finally, to the extent applicable, the AML Compliance Officer should report to a member of the Board of Directors (or other high level executive officer) on AML compliance issues. This senior officer or director should communicate with firm employees on AML issues to further demonstrate the firm's commitment to AML compliance. The firm's senior management should work with the AML Compliance Officer to help ensure that the firm's AML policies, procedures, and programs meet all applicable government standards and that they are effective in detecting, deterring, and punishing or correcting AML misconduct. The firm's senior management also should work with the AML Compliance Officer to ensure that the AML compliance policies, procedures, and programs are updated and reflect current requirements.

Establish An Ongoing Training Program

The Money Laundering Abatement Act requires firms to develop ongoing employee training programs on AML issues. The AML employee training should be developed under the leadership of the AML Compliance Officer or senior management. Educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos are all appropriate training vehicles for AML training. The training may vary based on the type of firm and its size, its customer base, and its resources. The NASD urges its members to instruct their employees about the following topics, at a minimum:

- how to identify "red flags" and possible signs of money laundering that could arise during the course of their duties;
- what to do once the risk is identified;
- what their roles are in the firm's compliance efforts;
- how to perform their roles;
- the firm's record retention policy; and
- disciplinary consequences, including civil and criminal penalties for non-compliance with the Money Laundering Abatement Act.

The NASD advises its members, *at a minimum*, to implement AML training on an annual basis. Frequent evaluation of training programs may be necessary to ensure that firms are informing employees about any new developments with the rules and regulations. As noted above, firms should update their training materials, as necessary, to reflect new developments in the law. Incorporation of money laundering compliance training into continuing education programs is recommended for both registered representatives and supervisors.

A broker/dealer should scrutinize its operations to determine if there are certain employees who may need additional or specialized training due to their duties and responsibilities. For example, employees in Compliance, Margin, and Corporate Security may need more comprehensive training. The firm should train these employees or have these employees receive the appropriate instruction to ensure compliance with the Money Laundering Abatement Act.

Establish An Independent Testing Function

In addition to the firm's overall supervisory responsibility to ensure that its procedures are being followed properly, broker/dealers must have an independent testing function to review and assess the adequacy of and level of compliance with the firm's AML compliance program. Either member personnel or a qualified outside party may perform the testing function, depending in part on the firm's size and resources. Smaller firms, for example, may consider using a qualified outside party to complete this function or they may find it more cost effective to use appropriately trained firm personnel. If a firm uses internal personnel, sufficient separation of functions should be maintained to ensure the independence of the internal testing personnel.

The independent testing should be performed annually. After a test is complete, the internal testing personnel or qualified outside party should report its findings to senior management or to an internal audit committee, as appropriate. The firm should ensure that there are procedures for implementation of any of the internal testing personnel's or third party's recommendations and corrective or disciplinary action as the case may warrant.

INTRODUCING BROKERS AND CLEARING BROKERS

The NASD wishes to emphasize that both introducing brokers and clearing brokers have responsibilities under the Money Laundering Abatement Act. **All** broker/dealers should devote special attention to potentially high-risk areas for money laundering. Both introducing brokers and clearing brokers must establish and implement the appropriate AML procedures identified above to comply with the Money Laundering Abatement Act's requirements.

In order to detect suspicious activity, it is imperative that introducing and clearing brokers work together to achieve compliance with the Money Laundering Abatement Act. For instance, introducing brokers generally are in the best position to "know the customer," and thus to identify potential money laundering concerns at the account opening stage, including verification of the identity of the customer and deciding whether to open an account for a customer.[40] In essence, introducing brokers should understand that they are the first line of defense in detecting and deterring suspicious activity. Clearing firms, in turn, may be in a better position to monitor customer transaction activity, including but not limited to, trading, wire transfers, and the deposit and withdrawal into and out of accounts of different financial instruments. To assist introducing brokers and, more importantly, satisfy their own obligations under federal law, clearing firms should establish both automated systems to detect suspicious activity and procedures to share AML information and responsibilities with introducing brokers, consistent with the Money Laundering Abatement Act. For example, both the introducing broker and clearing firm may have information concerning a customer relevant to an assessment of whether a wire transfer out of an account to a particular destination raises any AML concerns.

Importantly, introducing brokers must have a basis for assuring themselves that their clearing firms are monitoring customer account activity on their behalf. Similarly, clearing firms must have a basis for assuring themselves that their introducing firms are following appropriate customer identification procedures. Responsibilities relating to AML compliance should be clearly allocated between the parties, and such responsibilities should be specified in the parties' clearing agreements pursuant to NASD Rule 3230. Any such allocation, however, would not relieve either party from its independent obligation to comply with AML laws.

In short, introducing brokers and clearing firms need to work together to allow each firm to meet its obligation to comply with the AML laws.

CONCLUSION

As stated above, the NASD will update its guidance as new AML rules and regulations become final. In the interim, the NASD reminds members to comply with the provisions of the Money Laundering Abatement Act that currently apply to broker/dealers. Although the obligation to develop and implement an AML compliance program is not a “one-size-fits-all” requirement, all broker/dealers must have an AML compliance program designed to achieve compliance with the BSA and the regulations promulgated thereunder.

ENDNOTES

1 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

2 31 U.S.C. §§ 5311, *et seq*.

3 In its proposed rules released in December 2001, Treasury defines "correspondent account" for purposes of broker/dealers as "an account established to receive deposits from, make payments on behalf of a foreign bank, or handle other financial transactions related to such bank." *See* 66 Fed. Reg. 67,459 (December 28, 2001). The NASD will keep members apprised of any changes to the definition of "correspondent account" when Treasury releases its final rules in this area. Please also note that Treasury's definition is different from the definition of correspondent brokerage accounts.

4 *See* 66 Fed. Reg. 67,669 (December 31, 2001). NASD Regulation's AML Web Page provides links to Treasury's proposed and final regulations.

5 *See* 66 Fed. Reg. 67,459 (December 28, 2001).

6 *See* 67 Fed. Reg. 9873 (March 4, 2002); 67 Fed. Reg. 9879 (March 4, 2002).

7 *See generally Anti-Money Laundering, Efforts in the Securities Industry*, Report to the Chairman, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate, GAO-02-111 (October 2001).

8 Title 18 U.S.C. §§ 1956 and 1957 make knowingly engaging in, or attempting to engage in, financial transactions involving the proceeds of certain unlawful activities a criminal offense. Therefore, under the criminal statutes, a person or entity could be prosecuted for assisting or participating in money laundering perpetrated by its customer if the firm (or person) knew or was willfully blind to the fact that the transaction involved illegal funds. Criminal penalties include fines up to $500,000 or twice the value of the property involved in the transaction, whichever is greater, and prison sentences as long as 20 years. In addition to criminal penalties, violators may face civil penalties up to the greater of the value of the property, funds, or monetary interests involved in the transaction or $10,000, as well as forfeiture of any property involved in the transaction. The BSA also imposes criminal and civil penalties for violations of the BSA or its implementing regulations. Generally, a person can be subject to a criminal fine of up to $250,000 or imprisonment of up to 5 years, or both. A person who violates the BSA while violating another law of the United States, or engaging in a pattern of illegal activity, is subject to a criminal fine of up to $500,000 or imprisonment of up to 10 years, or both. The Money Laundering Abatement Act adds additional criminal and civil penalties that can be up to two times the amount of the transaction, not to exceed $1,000,000 for violations of certain BSA provisions.

9 *See NASD Notice to Members 89-12, Reporting Suspicious Currency and Other Questionable Transactions to the IRS/Customs Hotline*.

10 *See* note 3.

11 *See* 66 Fed. Reg. 67,459 (December 28, 2001).

12 *See* 67 Fed. Reg. 9873 (March 4, 2002); 67 Fed. Reg. 9879 (March 4, 2002).

13 *See* 67 Fed. Reg. 9873 (March 4, 2002); 67 Fed. Reg. 9879 (March 4, 2002).

14 *See* 66 Fed. Reg. 67,459 (December 28, 2001).

15 *See* 66 Fed. Reg. 67,669 (December 31, 2001).

16 *See* File No. SR-NASD-2002-24.

17 The U.S. Sentencing Commission Guidelines for organizations set out the following criteria for an effective corporate compliance program: (1) whether the company's compliance standards and procedures are reasonably capable of reducing the prospect of criminal activity; (2) whether there is oversight of the compliance program by high-level personnel; (3) whether the company exercises due care in delegating substantial authority; (4) whether the company communicates effectively to all levels of employees; (5) whether the company has in place viable systems for monitoring, auditing, and reporting suspected misconduct without fear of reprisal; (6) whether the company enforces compliance standards in a consistent manner using appropriate disciplinary measures; and (7) whether the company has taken reasonable steps to respond to and prevent further similar offenses upon detection of a violation. *See also In Re Caremark International Inc. Derivative Litigation,* 698 A.2d 959 (Del. Ch. 1996)*; McCall V. Scott,* 250 F. 3d 1997 (9th Cir. 2001).

18 The New York Stock Exchange (NYSE) has also proposed Rule 445, which mirrors the NASD's proposed rule. *See* File No. SR-NYSE-2002-10 (filed with the SEC on February 27, 2002).

19 31 U.S.C. § 5318(h) (amended by Section 352 of the Money Laundering Abatement Act).

20 *See USA Patriot Act of 2001: Consideration of H.R. 3162 Before the Senate* (October 25, 2001) (statement of Sen. Sarbanes); *Financial Anti-Terrorism Act of 2001: Consideration Under Suspension of Rules of H.R. 3004 Before the House of Representatives* (October 17, 2001) (statement of Rep. Kelly) (provisions of the Financial Anti-Terrorism Act of 2001 were incorporated as Title III in the PATRIOT Act.)

21 *See Notice to Members 96-32; Notice to Members 96-70; and Notice to Members 99-11*.

22 Treasury has until October 26, 2002 to promulgate additional customer identification requirements.

23 Firms should authenticate customer identity at the time of account opening, and not just when an account shows suspicious activity.

24 *See Notice to Members 01-67, Terrorist Activity*. Executive Order 13224 prohibits transactions with those persons and organizations listed on the OFAC Web Site on the SDN List as well as with the listed embargoed countries and regions; *See also* Section 326 of the Money Laundering Abatement Act. The OFAC Web Site is updated frequently, so members should consult the list on a regular basis. Software programs that allow firms to perform this function in a more user friendly and automated manner are available.

25 Note that under the BSA, firms must record a current passport number or other valid government identification number for transfers or transmittals of $3,000 or more by or for non-resident alien accounts. *See* 31 C.F.R. 103.33 (2001).

26 31 U.S.C. § 5318(k) (amended by Section 319(b) of the Money Laundering Abatement Act).

27 31 U.S.C. § 5318(j) (amended by Section 313 of the Money Laundering Abatement Act). Please note that Treasury included a model certification form in its December 2001 rule proposal, available at *www.nasdr.com /money.asp*.

28 31 U.S.C. § 5318(i) (amended by Section 312 of the Money Laundering Abatement Act).

29 Treas. Dept., Bd. of Gov. of Fed. Res., Comp. Of the Currency, F.D.I.C., O.T.S. and State Dept., *Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption*, (Jan. 2001) and at *www.ustreas.gov/press/ releases/guidance.htm*.

30 31 U.S.C. § 5318(i) (amended by Section 312(a)(i)(4)(B) of the Money Laundering Abatement Act).

31 31 U.S.C. § 5318(i) (amended by Section 312(a)(i)(3) of the Money Laundering Abatement Act).

32 31 U.S.C. § 5318(g).

33 Evidence that a broker/dealer knows that the property involved in a financial transaction constitutes the proceeds of unlawful activity and nonetheless conducts (or attempts to conduct) the financial transaction with the unlawful proceeds with the intent to promote the unlawful activity or knowing that the transaction is designed to conceal or disguise the nature, source, or ownership of the unlawful proceeds, can subject a broker/dealer to criminal prosecution. *See* 18 U.S.C. § 1956.

34 66 Fed. Reg. 67,669 at 67,674 (Dec. 31, 2001).

35 Firms are also reminded to notify self-regulatory organizations and the SEC if they detect indicators of securities laws violations. Firms should note that there are exceptions to the proposed broker/dealer SAR requirements, including that a broker/ dealer is not required to file a SAR to report a possible violation of any of the federal securities laws or rules of a self-regulatory organization by the broker/dealer or any of its officers or directors, employees, or other registered representatives, other than certain rules, so long as such violation is properly reported to the SEC or a self-regulatory organization. *See* 66 Fed. Reg. 67,669 at 67,676-677 (Dec. 31, 2001).

36 The FATF is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering. The FATF monitors members' progress in implementing anti-money laundering measures, reviews money laundering techniques and counter-measures, and promotes the adoption and implementation of anti-money laundering measures globally. *See* links to the FATF Web Site at *www.nasdr.com/money.asp*.

37 *See* Speech by Lori Richards, Director of Securities and Exchange Commission's Office of Compliance Inspections and Examinations, *Money Laundering: It's on the SEC's Radar Screen* (May 8, 2001); *See also* SIA, *Preliminary Guidance for Deterring Money Laundering Activity*, at 12-13 (Feb. 2002); Sarah B. Estes, Sutherland, Asbill & Brennan LLP, *Securities Broker-Dealers and Money Laundering: The Obligations of Broker-Dealers Under Money Laundering Laws* at 5-6 (2001).

38 Firms may wish to consult FinCEN's Web Site for more information (*see www.treas.gov.fincen*), including, annual SAR Activity Review reports and SAR Bulletins, which discuss trends in suspicious activity reporting and give helpful tips.

39 *See* 67 Fed. Reg. 9873 (March 4, 2002).

40 All broker/dealers should consider using electronic databases (such as Equifax, Experion, Lexis/Nexis, or other in-house or custom databases) to verify customer identity.

Regulatory Notice 19-18

Anti-Money Laundering (AML) Program

FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations

May 6, 2019

Notice Type
- Guidance

Suggested Routing
- Compliance
- Legal
- Operations
- Senior Management

Key Topics
- Anti-Money Laundering
- Compliance Programs

Referenced Rules & Notices
- Bank Secrecy Act
- FINRA Rule 3310
- Notice to Members 02-21

Summary

FINRA is issuing this *Notice* to provide guidance to member firms regarding suspicious activity monitoring and reporting obligations under FINRA Rule 3310 (Anti-Money Laundering Compliance Program).

Questions concerning this *Notice* should be directed to:

- Victoria Crane, Associate General Counsel, Office of General Counsel, at (202) 728-8104 or *victoria.crane@finra.org*; or
- Blake Snyder, Senior Director, Member Regulation, at (561) 443-8051 or *blake.snyder@finra.org*.

Background and Discussion

FINRA Rule 3310 (Anti-Money Laundering Compliance Program) requires each member firm to develop and implement a written anti-money laundering (AML) program reasonably designed to achieve and monitor the firm's compliance with the requirements of the Bank Secrecy Act (BSA),[1] and the implementing regulations promulgated thereunder by the Department of the Treasury (Treasury).

FINRA Rule 3310(a) requires firms to "[e]stablish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of transactions required under [the BSA] and the implementing regulation thereunder." The BSA authorizes Treasury to require that financial institutions file suspicious activity reports (SARs).[2]

FINRA
Financial Industry Regulatory Authority

Under Treasury's SAR rule,[3] a broker-dealer must report a transaction to the Financial Crimes Enforcement Network (FinCEN) if it is conducted or attempted by, at or through a broker-dealer, it involves or aggregates funds or other assets of at least $5,000, and the broker-dealer knows, suspects or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

- 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;
- is designed, whether through structuring or other means, to evade any regulations promulgated under the BSA;
- 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 broker-dealer knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- involves use of the broker-dealer to facilitate criminal activity.[4]

Broker-dealers must report the suspicious activity by completing a SAR and filing it in accordance with the requirements of Treasury's SAR rule.[5] Broker-dealers must maintain a copy of any SAR filed and supporting documentation for a period of five years from the date of filing the SAR.[6] FinCEN has provided guidance[7] to the industry advising that if the activity that was the subject of a SAR filing continues, firms should review any continuing activity at least every 90 days to consider whether a continuing activity SAR filing is warranted, with the filing deadline being 120 days after the date of the previously related SAR filing.

In situations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, broker-dealers must immediately notify by telephone an appropriate law enforcement authority in addition to filing timely a SAR. The firm may call FinCEN's Hotline at (866) 556-3974.

Money Laundering Red Flags

FINRA published a list of "money laundering red flags" in *Notice to Members 02-21* (NTM 02-21). Since NTM 02-21 was published, guidance detailing additional red flags that may be applicable to the securities industry have been published by a number of U.S. government agencies and international organizations.[8] FINRA is issuing this *Notice* to provide examples of these additional money laundering red flags for firms to consider incorporating into their AML programs, as may be appropriate in implementing a risk-based approach to BSA/AML compliance. This could include, as applicable, incorporation into policies and procedures relating to suspicious activity monitoring or suspicious activity investigation

and SAR reporting. Upon detection of red flags through monitoring, firms should consider whether additional investigation, customer due diligence measures or a SAR filing may be warranted.

The following is not an exhaustive list and does not guarantee compliance with AML program requirements or provide a safe harbor from regulatory responsibility. Further, it is important to note that a red flag is not necessarily indicative of suspicious activity, and that not every item identified in this *Notice* will be relevant for every broker-dealer, every customer relationship or every business activity.

Firms should also be aware of emerging areas of risk, such as risks associated with activity in digital assets. Regardless of whether such assets are securities, BSA/AML requirements, including SAR filing requirements apply, and firms should thus consider the relevant risks, monitor for suspicious activity and, as applicable, report any such activity.

This *Notice* is intended to assist broker-dealers in complying with their existing obligations under BSA/AML requirements and does not create any new requirements or expectations. In addition, this *Notice* incorporates the red flags listed in NTM 02-21 so that firms can refer to this *Notice* only for examples of potential red flags.

I. Potential Red Flags in Customer Due Diligence and Interactions With Customers

1. The customer provides the firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. Or, the customer provides information that is inconsistent with other available information about the customer. This indicator may apply to account openings and to interaction subsequent to account opening.
2. The customer is reluctant or refuses to provide the firm with complete customer due diligence information as required by the firm's procedures, which may include information regarding the nature and purpose of the customer's business, prior financial relationships, anticipated account activity, business location and, if applicable, the entity's officers and directors.
3. The customer refuses to identify a legitimate source of funds or information is false, misleading or substantially incorrect.
4. The customer is domiciled in, doing business in or regularly transacting with counterparties in a jurisdiction that is known as a bank secrecy haven, tax shelter, high-risk geographic location (*e.g.*, known as a narcotics producing jurisdiction, known to have ineffective AML/Combating the Financing of Terrorism systems) or conflict zone, including those with an established threat of terrorism.
5. The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
6. The customer has no discernable reason for using the firm's service or the firm's location (*e.g.*, the customer lacks roots to the local community or has gone out of his or her way to use the firm).

7. The customer has been rejected or has had its relationship terminated as a customer by other financial services firms.
8. The customer's legal or mailing address is associated with multiple other accounts or businesses that do not appear related.
9. The customer appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.
10. The customer is a trust, shell company or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.
11. The customer is publicly known or known to the firm to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds, or is known to associate with such persons. Sources for this information could include news items, the Internet or commercial database searches.
12. The customer's background is questionable or differs from expectations based on business activities.
13. The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent business or other purpose.
14. An account is opened by a politically exposed person (PEP),[9] particularly in conjunction with one or more additional risk factors, such as the account being opened by a shell company[10] beneficially owned or controlled by the PEP, the PEP is from a country which has been identified by FATF as having strategic AML regime deficiencies, or the PEP is from a country known to have a high level of corruption.
15. An account is opened by a non-profit organization that provides services in geographic locations known to be at higher risk for being an active terrorist threat.[11]
16. An account is opened in the name of a legal entity that is involved in the activities of an association, organization or foundation whose aims are related to the claims or demands of a known terrorist entity.[12]
17. An account is opened for a purported stock loan company, which may hold the restricted securities of corporate insiders who have pledged the securities as collateral for, and then defaulted on, purported loans, after which the securities are sold on an unregistered basis.
18. An account is opened in the name of a foreign financial institution, such as an offshore bank or broker-dealer, that sells shares of stock on an unregistered basis on behalf of customers.
19. An account is opened for a foreign financial institution that is affiliated with a U.S. broker-dealer, bypassing its U.S. affiliate, for no apparent business purpose. An apparent business purpose could include access to products or services the U.S. affiliate does not provide.

II. Potential Red Flags in Deposits of Securities

1. A customer opens a new account and deposits physical certificates, or delivers in shares electronically, representing a large block of thinly traded or low-priced securities.
2. A customer has a pattern of depositing physical share certificates, or a pattern of delivering in shares electronically, immediately selling the shares and then wiring, or otherwise transferring out the proceeds of the sale(s).
3. A customer deposits into an account physical share certificates or electronically deposits or transfers shares that:
   - were recently issued or represent a large percentage of the float for the security;
   - reference a company or customer name that has been changed or that does not match the name on the account;
   - were issued by a shell company;
   - were issued by a company that has no apparent business, revenues or products;
   - were issued by a company whose SEC filings are not current, are incomplete, or nonexistent;
   - were issued by a company that has been through several recent name changes or business combinations or recapitalizations;
   - were issued by a company that has been the subject of a prior trading suspension; or
   - were issued by a company whose officers or insiders have a history of regulatory or criminal violations, or are associated with multiple low-priced stock issuers.
4. The lack of a restrictive legend on deposited shares seems inconsistent with the date the customer acquired the securities, the nature of the transaction in which the securities were acquired, the history of the stock or the volume of shares trading.
5. A customer with limited or no other assets at the firm receives an electronic transfer or journal transfer of large amounts of low-priced, non-exchange-listed securities.
6. The customer's explanation or documents purporting to evidence how the customer acquired the shares does not make sense or changes upon questioning by the firm or other parties. Such documents could include questionable legal opinions or securities purchase agreements.
7. The customer deposits physical securities or delivers in shares electronically, and within a short time-frame, requests to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.
8. Seemingly unrelated clients open accounts on or at about the same time, deposit the same low-priced security and subsequently liquidate the security in a manner that suggests coordination.

III. Potential Red Flags in Securities Trading[13]

1. The customer, for no apparent reason or in conjunction with other "red flags," engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" stocks and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
2. There is a sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security.
3. The customer's activity represents a significant proportion of the daily trading volume in a thinly traded or low-priced security.
4. A customer buys and sells securities with no discernable purpose or circumstances that appear unusual.
5. Individuals known throughout the industry to be stock promoters sell securities through the broker-dealer.
6. A customer accumulates stock in small increments throughout the trading day to increase price.
7. A customer engages in pre-arranged or other non-competitive securities trading, including wash or cross trades, with no apparent business purpose.
8. A customer attempts to influence the closing price of a stock by executing purchase or sale orders at or near the close of the market.
9. A customer engages in transactions suspected to be associated with cyber breaches of customer accounts, including potentially unauthorized disbursements of funds or trades.
10. A customer engages in a frequent pattern of placing orders on one side of the market, usually inside the existing National Best Bid or Offer (NBBO), followed by the customer entering orders on the other side of the market that execute against other market participants that joined the market at the improved NBBO (activity indicative of "spoofing").
11. A customer engages in a frequent pattern of placing multiple limit orders on one side of the market at various price levels, followed by the customer entering orders on the opposite side of the market that are executed and the customer cancelling the original limit orders (activity indicative of "layering").
12. Two or more unrelated customer accounts at the firm trade an illiquid or low-priced security suddenly and simultaneously.
13. The customer makes a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security.

14. The customer is known to have friends or family who work at or for the securities issuer, which may be a red flag for potential insider trading or unlawful sales of unregistered securities.
15. The customer's purchase of a security does not correspond to the customer's investment profile or history of transactions (*e.g.*, the customer may never have invested in equity securities or may have never invested in a given industry, but does so at an opportune time) and there is no reasonable explanation for the change.
16. The account is using a master/sub structure, which enables trading anonymity with respect to the sub-accounts' activity, and engages in trading activity that raises red flags, such as the liquidation of microcap issuers or potentially manipulative trading activity.
17. The firm receives regulatory inquiries or grand jury or other subpoenas concerning the firm's customers' trading.
18. The customer engages in a pattern of transactions in securities indicating the customer is using securities to engage in currency conversion. For example, the customer delivers in and subsequently liquidates American Depository Receipts (ADRs) or dual currency bonds for U.S. dollar proceeds, where the securities were originally purchased in a different currency.
19. The customer engages in mirror trades or transactions involving securities used for currency conversions, potentially through the use of offsetting trades.
20. The customer appears to buy or sell securities based on advanced knowledge of pending customer orders.

IV. Potential Red Flags in Money Movements

1. The customer attempts or makes frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies and procedures relating to the deposit of cash and cash equivalents.
2. The customer "structures" deposits, withdrawals or purchases of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements, and may state directly that they are trying to avoid triggering a reporting obligation or to evade taxing authorities.
3. The customer seemingly breaks funds transfers into smaller transfers to avoid raising attention to a larger funds transfer. The smaller funds transfers do not appear to be based on payroll cycles, retirement needs, or other legitimate regular deposit and withdrawal strategies.
4. The customer's account shows numerous currency, money order (particularly sequentially numbered money orders) or cashier's check transactions aggregating to significant sums without any apparent business or lawful purpose.

5. The customer frequently changes bank account details or information for redemption proceeds, in particular when followed by redemption requests.
6. The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
7. Wire transfers are made in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
8. Incoming payments are made by third-party checks or checks with multiple endorsements.
9. Outgoing checks to third parties coincide with, or are close in time to, incoming checks from other third parties.
10. Payments are made by third party check or money transfer from a source that has no apparent connection to the customer.
11. Wire transfers are made to or from financial secrecy havens, tax havens, high-risk geographic locations or conflict zones, including those with an established presence of terrorism.
12. Wire transfers originate from jurisdictions that have been highlighted in relation to black market peso exchange activities.
13. The customer engages in transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (*e.g.*, countries designated by national authorities, such as FATF, as non-cooperative countries and territories).
14. The parties to the transaction (*e.g.*, originator or beneficiary) are from countries that are known to support terrorist activities and organizations.
15. Wire transfers or payments are made to or from unrelated third parties (foreign or domestic), or where the name or account number of the beneficiary or remitter has not been supplied.
16. There is wire transfer activity that is unexplained, repetitive, unusually large, shows unusual patterns or has no apparent business purpose.
17. The securities account is used for payments or outgoing wire transfers with little or no securities activities (*i.e.*, account appears to be used as a depository account or a conduit for transfers, which may be purported to be for business operating needs).
18. Funds are transferred to financial or depository institutions other than those from which the funds were initially received, specifically when different countries are involved.

19. The customer engages in excessive journal entries of funds between related or unrelated accounts without any apparent business purpose.
20. The customer uses a personal/individual account for business purposes or vice versa.
21. A foreign import business with U.S. accounts receives payments from outside the area of its customer base.
22. There are frequent transactions involving round or whole dollar amounts purported to involve payments for goods or services.
23. Upon request, a customer is unable or unwilling to produce appropriate documentation (*e.g.*, invoices) to support a transaction, or documentation appears doctored or fake (*e.g.*, documents contain significant discrepancies between the descriptions on the transport document or bill of lading, the invoice, or other documents such as the certificate of origin or packing list).
24. The customer requests that certain payments be routed through nostro[14] or correspondent accounts held by the financial intermediary instead of its own accounts, for no apparent business purpose.
25. Funds are transferred into an account and are subsequently transferred out of the account in the same or nearly the same amounts, especially when the origin and destination locations are high-risk jurisdictions.
26. A dormant account suddenly becomes active without a plausible explanation (*e.g.*, large deposits that are suddenly wired out).
27. Nonprofit or charitable organizations engage in financial transactions 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.
28. There is unusually frequent domestic and international automated teller machine (ATM) activity.
29. A person customarily uses the ATM to make several deposits into a brokerage account below a specified BSA/AML reporting threshold.
30. Many small, incoming wire transfers or deposits are made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history; the checks or money orders may reference in a memo section "investment" or "for purchase of stock." This may be an indicator of a Ponzi scheme or potential funneling activity.
31. Wire transfer activity, when viewed over a period of time, reveals suspicious or unusual patterns, which could include round dollar, repetitive transactions or circuitous money movements.

V. Potential Red Flags in Insurance Products

1. The customer cancels an insurance contract and directs that the funds be sent to a third party.
2. The customer deposits an insurance annuity check from a cancelled policy and immediately requests a withdrawal or transfer of funds.
3. The customer cancels an annuity product within the free-look period. This could be a red flag if accompanied with suspicious indicators, such as purchasing the annuity with several sequentially numbered money orders or having a history of cancelling annuity products during the free-look period.
4. The customer opens and closes accounts with one insurance company, then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.
5. The customer purchases an insurance product with no concern for the investment objective or performance.

VI. Other Potential Red Flags

1. The customer is reluctant to provide information needed to file reports to proceed with the transaction.
2. The customer exhibits unusual concern with the firm's compliance with government reporting requirements and the firm's AML policies.
3. The customer tries to persuade an employee not to file required reports or not to maintain the required records.
4. Notifications received from the broker-dealer's clearing firm that the clearing firm had identified potentially suspicious activity in customer accounts. Such notifications can take the form of alerts or other concern regarding negative news, money movements or activity involving certain securities.
5. Law enforcement has issued subpoenas or freeze letters regarding a customer or account at the securities firm.
6. The customer makes high-value transactions not commensurate with the customer's known income or financial resources.
7. The customer wishes to engage in transactions that lack business sense or an apparent investment strategy, or are inconsistent with the customer's stated business strategy.
8. The stated business, occupation or financial resources of the customer are not commensurate with the type or level of activity of the customer.
9. The customer engages in transactions that show the customer is acting on behalf of third parties with no apparent business or lawful purpose.

10. The customer engages in transactions that show a sudden change inconsistent with normal activities of the customer.
11. Securities transactions are unwound before maturity, absent volatile market conditions or other logical or apparent reason.
12. The customer does not exhibit a concern with the cost of the transaction or fees (*e.g.*, surrender fees, or higher than necessary commissions).
13. A borrower defaults on a cash-secured loan or any loan that is secured by assets that are readily convertible into currency.
14. There is an unusual use of trust funds in business transactions or other financial activity.

Endnotes

1. 31 U.S.C. 5311, *et seq*.
2. *See* 31 U.S.C. 5318(g).
3. *See* 31 CFR 1023.320.
4. *See* 31 CFR 1023.320(a)(2).
5. *See* 31 CFR 1023.320.
6. *See* 31 CFR 1023.320(d).
7. *See* FinCEN SAR Activity Review Issue 21 (May 2012).
8. *See, e.g*, Financial Action Task Force (FATF), Guidance for a Risk-Based Approach for the Securities Sector, October 2018; FATF, Money Laundering and Terrorist Financing in the Securities Sector, October 2009; FATF, Guidance for Financial Institutions in Detecting Terrorist Financing, April 2002; FATF Report, Laundering the Proceeds of Corruption, July 2011; FATF Report, Risk of Terrorist Abuse in Non-Profit Organisations, June 2014; FinCEN Advisory FIN-2010-A001: Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade Based Money Laundering, February 2010; U.S. Department of State, Money Laundering Methods, Trends and Typologies, March 2004; Securities and Exchange Commission (SEC) National Exam Risk Alert on Master/Sub-accounts, September 2011; SEC National Exam Risk Alert on Broker-Dealer Controls Regarding Customer Sales of Microcap Securities, October 2014; and SEC Responses to Frequently Asked Questions about a Broker-Dealer's Duties When Relying on the Securities Act Section 4(a)(4) Exemption to Execute Customer Orders, October 2014. *See also Regulatory Notices 09-05* (January 2009) and *10-18* (April 2010); and Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering, Money Laundering and Terrorist Financing "Red Flags."
9. A "Politically Exposed Person" is defined by FATF as an individual who is or has been entrusted with a prominent public function, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, or important political party officials. *See* FATF Guidance, Politically Exposed Persons, June 2013.
10. A "shell company" is an issuer of securities for which a registration statement has been filed with the SEC that has: (1) no or nominal operations; and (2) either: (i) no or nominal assets; (ii) assets consisting solely of cash and cash equivalents; or (iii) assets consisting of any amount of cash or cash equivalents and nominal other assets. *See* 17 CFR 230.504.
11. The FATF Report on Risk of Terrorist Abuse in Non-Profit Organisations (FATF Report), June 2014, defines "terrorist threat" as: A person or group of people, object or activity, with the potential to cause harm. Threat is contingent on actors that possess both the capability and intent to do harm.
12. The FATF Report defines "terrorist entity" as a terrorist and/or terrorist organization identified as a supporter of terrorism by national or international sanctions lists, or assessed by a jurisdiction as active in terrorist activity. *See id*.
13. These red flags could also be indicative of securities law violations.
14. Nostro accounts are accounts that a financial institution holds in a foreign currency in another bank, typically in order to facilitate foreign exchange transactions.