Common Examination Findings and Effective Compliance Practices (Small Firm Focus)
Tuesday, May 22
10:00 a.m. – 11:00 a.m.

Join FINRA staff as they discuss FINRA's examination process and most common deficiencies noted during cycle examinations of small firms. Industry practitioners discuss effective practices for preparing for examinations taking corrective action and updating compliance procedures and practices based on lessons learned from common examination findings.

Moderator:
Lance Burkett
District Director, Sales Practice
FINRA Denver District Office

Panelists:
Stephen Kohn
President and Chief Executive Officer
Stephen A. Kohn & Associates, Ltd.

Elizabeth Page
Vice President and Director
FINRA Boston District Office

Harry Striplin
Chief Compliance Officer
Umpqua Investments, Inc.

© 2018 Financial Industry Regulatory Authority, Inc. All rights reserved.

Common Examination Findings and Effective Compliance Practices (Small Firm Focus) Panelist Bios:

Moderator:

Lance Burkett, District Director, FINRA Denver Office, began his securities industry career in 1993 as a Securities Fraud Investigator for the State of Arizona Securities Division, working exclusively on fraud cases involving broker-dealers. Later, at a FINRA member firm, he was responsible for supervising Producing Branch Managers and Field Representatives as the Field Compliance Director. Throughout his tenure with FINRA, Mr. Burkett has held positions ranging from Compliance Examiner, responsible for examining FINRA member firms for general compliance, to District Director, responsible for the management and oversight of the regulatory programs within the Denver District office. In addition to his regulatory responsibilities, Mr. Burkett earned his Certified Regulatory and Compliance Professional™ designation through the FINRA Institute at Wharton and has developed content and presented at several FINRA Institute class offerings.

Panelists:

Stephen Kohn has been employed in the financial services industry since 1984, to which he has devoted most of his working life. Founded in 1996, Mr. Kohn owns and operates a FINRA small member firm, Stephen A. Kohn & Associates, Ltd. (SAKL) located in Lakewood, Colorado. SAKL is a small, full service, independent broker/dealer, catering to the needs of 28 independent representatives and their clients, with office locations in seven states, registered in 35. Mr. Kohn has been elected, by the Small Firm Membership, to the FINRA Board of Governors, to represent their interests and issues at the highest levels. Mr. Kohn has been twice elected to the National Adjudicatory Council (NAC) by FINRA's small firms, first in 2009 and again in 2014. His second term on the NAC, as one of two small firm members, runs until the end of 2017. The NAC is FINRA's appellate division, hearing appeals to enforcement decisions and other issues. Mr. Kohn serves on the NAC's Sanction Guideline Review and Revision Sub-Committee. This sub-committee has been convened to review the guidelines, ensure that sanctions in appeals that are upheld by the NAC are fair and appropriate and to recommend revisions to the Sanction Guidelines as needed. He is also an industry arbitrator and currently serves on the District 3 Committee. In his more than three decades in the Securities Industry, Mr. Kohn has been employed at a plethora of large and small firms as well as his own. Of all the firms at which he has been employed, only two are still in business and one of them is Stephen A. Kohn & Associates, Ltd. Mr. Kohn holds the following securities licenses: Series, 7, 24, 53, 63, 72, 73, 79 and 99. He graduated from C.W. Post College of Long Island University in 1964 with a BA degree. He has also served in the U.S. Coast Guard.

Elizabeth Page is Vice President and Director of FINRA's Boston District office. In this role, she is responsible for the regulatory programs that oversee the FINRA firms and registered representatives within New England and portions of Canada and Europe. Prior to her position in Boston, Ms. Page was the Deputy Director in the FINRA's Chicago District office and has served in a variety of staff and management roles including managing and conducting onsite examinations of the main offices and branches of FINRA firms, investigations of customer complaints and terminations for cause and applications for membership. Ms. Page has a Bachelor degree in Finance and a Master of Business Administration degree from the University of Denver.

Harry Striplin is Chief Compliance Officer for Umpqua Investments, Inc., a small firm headquartered in Portland, Oregon. He has been with Umpqua Investments for nine years. Mr. Striplin has more than 36 years of experience working at small firms and more than 27 years serving as a Chief Compliance Officer in the small firm environment. He has served as a member of FINRA's District 3 Committee, the Securities Industry Regulatory Council on Continuing Education and has been a panelist at FINRA securities conferences. Mr. Striplin has been a member of the Securities Industry Continuing Education Content Committee for more than 20 years. Mr. Striplin serves as an arbitrator for FINRA Dispute Resolutions and has achieved his Certified Regulatory and Compliance Professional™ (CRCP™) certification through the FINRA Institute at Wharton.

© 2018 Financial Industry Regulatory Authority, Inc. All rights reserved.



2018 FINRA Annual Conference

May 21 – 23, 2018 • Washington, DC

Common Examination Findings and Effective Compliance Practices (Small Firm Focus)

FINRA

Panelists

- **Moderator**
  - Lance Burkett, District Director, Sales Practice, FINRA Denver District Office
- **Panelists**
  - Stephen Kohn, President and Chief Executive Officer, Stephen A. Kohn & Associates, Ltd.
  - Elizabeth Page, Vice President and Director, FINRA Boston District Office
  - Harry Striplin, Chief Compliance Officer, Umpqua Investments, Inc.

© 2018 FINRA. All rights reserved.

To Access Polling

- Under the “Schedule” icon on the home screen,
- Select the day,
- Choose the Common Examination Findings and Effective Compliance Practices (Small Firm Focus) session,
- Click on the polling icon: 

 | © 2018 FINRA. All rights reserved.

Polling Question 1

1. How does your firm utilize the FINRA Examination Findings Report?
   a. To keep up to date on what FINRA is finding within the Examination Program
   b. Utilize the Examination Findings Report to assess my firm's supervisory procedures and controls
   c. I have not reviewed or utilized the Examination Findings Report

© 2018 FINRA. All rights reserved.

Topics for Discussion

- FINRA Examination Program
- Report on FINRA Examination Findings
- Discussion on Common Findings
- Questions

© 2018 FINRA. All rights reserved.



Report on FINRA Examination Findings

DECEMBER 2017

CONTENTS

Highlighted Observations 2

Cybersecurity 2

Outside Business Activities and Private Securities Transactions 4

Anti-Money Laundering Compliance Program 5

Product Suitability 6

Best Execution 8

Market Access Controls 9

Summary of Additional Observations 11

Alternative Investments Held in Individual Retirement Accounts (IRAs) 11

Net Capital and Credit Risk Assessments 11

Order Capacity 12

Regulation SHO 13

TRACE Reporting 13

A REPORT FROM **THE FINANCIAL INDUSTRY REGULATORY AUTHORITY**

FINRA's examination program plays a central role in supporting FINRA's mission of investor protection and market integrity. A main component of this program is FINRA's examinations of broker-dealers ("firms" or "members") that are conducted on a regular cycle basis: each firm is examined at least once every four years, and many are examined even more frequently. In connection with each of these examinations, FINRA prepares a report—which is available only to the relevant firm—addressing certain aspects of the firm's compliance with securities rules and regulations. Firms are required to address issues identified by FINRA, and many do so by proactively taking corrective action before FINRA concludes its exam. Through this sort of rapid remediation, firms strengthen their compliance and supervisory programs, which ultimately helps better protect investors and the integrity of the markets.

FINRA is issuing this report as another resource that firms can use to strengthen their compliance with securities rules and regulations. Some firms have requested that FINRA make generally available a summary of observations from the cycle examination program, so that they can further improve their compliance functions based on the experiences of other firms, and better anticipate and address potential areas of concern well before their own cycle examinations.

This report focuses on selected observations from recent examinations that FINRA considers worth highlighting due to their potential impact on investors and markets or the frequency with which they occur. This report does not represent a complete inventory of observations about the industry as a whole, does not imply that any issues discussed exist at any particular firms, and should not be read as creating new legal or regulatory requirements or new interpretations of existing requirements. An individual firm may not have any deficiencies in the risk areas identified in the report.

This report also describes certain practices that FINRA has observed to be effective in appropriate circumstances, which other firms may be able to use as a resource in tailoring their compliance and supervisory programs to their business. There should be no inference, however, that FINRA requires firms to implement any specific practices described in this report that extend beyond the requirements of existing securities rules and regulations.

FINRA expects that this report will evolve over time as we work to ensure that it is helpful in supporting firms' compliance and supervisory efforts. FINRA welcomes feedback on how we could make future reports on examination findings more useful. If you have suggestions, please contact Daniel M. Sibears, Executive Vice President, Regulatory Operations/Shared Services, at (202) 728-6911; or Steven Polansky, Senior Director, Regulatory Operations/Shared Services, at (202) 728-8331.

Highlighted Observations

Cybersecurity

Cybersecurity is one of the principal operational risks facing broker-dealers. Recent revelations regarding successful attacks at a number of different entities underscore the need for firms to be vigilant in addressing cybersecurity threats. FINRA has focused on sharing information to help firms better protect their customers and themselves, including through recommendations offered in connection with an examination.[1] The primary federal securities law provision governing a firm's cybersecurity program is SEC Rule 30 of Regulation S-P, which requires firms to have written policies and procedures addressing the safeguarding of customer information and records.

FINRA has seen a significant increase in firms' attention to cybersecurity challenges over the past two years, including at the executive management level. Awareness about cybersecurity risk has increased substantially. Most firms we examined have established, or were establishing, risk management practices, although the quality of those practices varied substantially both within and across firms. In some cases, firms adopted and executed, on an ongoing basis, formal risk management practices that executive management approved and applied on a consistent, firmwide basis. And some of the firms we regulate are leaders in developing and adopting cutting-edge cybersecurity practices.

Firms with effective cybersecurity programs typically established strong governance structures and processes (scaled to the firm) that addressed cybersecurity in a risk management context. Firms escalated risk acceptance decisions and problems to the appropriate levels for resolution, as well as to inform future program development. Measures firms implemented included regular risk assessments with detailed, time-bound follow-up action plans to resolve higher-risk concerns. Firms supported these assessments with regular vulnerability and penetration tests. Firms also required employees to participate in regular, role-specific and generic cybersecurity training and testing, for example, through phishing email exercises. Firms with branch offices developed and implemented robust branch cybersecurity reviews as part of their branch examination programs. As appropriate to their scale, some firms implemented security information and event management, system usage behavior analytics and data loss prevention tools to identify, monitor, and address potentially anomalous or suspicious activity on their networks.

Selected Examination Findings

As the nature and sophistication of cybersecurity threats continue to evolve, even robust cybersecurity programs can be compromised when, for example, an employee opens an email attachment that contains malware. Common threats FINRA observed in 2016 and 2017 include phishing and spearphishing attacks,[2] ransomware attacks and fraudulent third-party wires that frequently involve use of email or stolen customer or financial advisor credentials.

FINRA observed a variety of areas where some firms could improve their cybersecurity programs against these and other threats.[3] These areas include:

- **Access Management –** Some firms FINRA examined did not address basic access management issues such as terminating departing employees' access to firm systems on a timely basis. In the case of privileged systems users, some firms did not implement procedures to log, monitor and supervise their activities to detect anomalies such as a privileged user assigning herself or himself extra access rights, performing unauthorized work during off-hours or logging in from different geographic locations concurrently.[4]
- **Risk Assessments –** Some firms did not have formal processes to conduct ongoing risk assessments of their data, systems and applications, and could not effectively identify their critical assets and the potential risks to those assets.
- **Vendor Management –** Some firms did not have formal processes to review a prospective vendor's cybersecurity preparedness or to ensure new vendors have appropriate protections in place. For example, some firms' contracts with vendors did not address key questions such as the vendor's responsibilities regarding notification to the firm in the event of a breach of customer or firm data. In cases where firms contracted with a parent organization for cybersecurity services, the parent's cybersecurity responsibilities were not sufficiently documented, such as in a service-level agreement.
- **Branch Offices –** FINRA found that firms' branch offices typically faced greater challenges in managing passwords, implementing patches and software updates, updating anti-virus software, controlling removable storage devices, encrypting data and reporting incidents.
- **Segregation of Duties –** FINRA observed some medium- and small-sized firms that did not segregate the responsibilities for requesting, implementing, and approving cybersecurity rules and systems changes. For example, some firms allowed application developers to access sensitive data in production systems and in some cases implement application code into production without appropriate oversight. In other cases, network engineers performed cybersecurity and information security functions without formal management oversight.
- **Data Loss Prevention –** FINRA observed that while larger- and medium-sized firms had implemented data loss prevention tools, there were opportunities to strengthen those implementations, including broadening rules that prevent transmission of Social Security numbers to include additional sensitive data such as customer account numbers; establishing thresholds to flag or block large file transfers to outside and untrusted recipients; and implementing formal change-management processes for data loss prevention system rule changes.

Outside Business Activities and Private Securities Transactions

FINRA Rules 3270 and 3280 require registered representatives to notify their firms of proposed outside business activities (OBAs), and all associated persons to notify their firms of proposed private securities transactions (PSTs), so firms can determine whether to limit or allow those activities to proceed. Certain OBAs and PSTs could potentially involve misconduct or create conflicts of interest that may expose both firms and customers to potential risks. The notifications required in the rules assist firms in identifying and determining how to mitigate those risks, including by placing conditions on, or prohibiting, participation in the proposed OBA or PST.[5]

Firms that had effective programs to manage OBAs and PSTs typically implemented proactive compliance efforts, particularly at the branch level. Firms used frequent training to make registered or associated persons aware of their responsibilities with respect to OBAs and PSTs, including the requirements to provide a firm prior written notice of a proposed activity. Firms also required these individuals to complete open-ended questionnaires and attestations regarding their involvement—or potential involvement—in OBAs and PSTs on a regular basis. Firms implemented various tools to identify individuals involved in undeclared OBAs and PSTs, including monitoring correspondence, fund movements, marketing materials, employee online activities and customer complaints. This also included monitoring for evidence of involvement in OBAs or PSTs the firm had prohibited.

Selected Examination Findings

FINRA observed instances in all sizes of retail brokerage firms in which registered persons, other associated persons or firms failed to meet one or more of their obligations under the rules. These instances include problems related to:

- **Notice –** FINRA observed that some individuals failed to notify their firms of proposed OBAs or PSTs, including situations where a new hire or current registered or associated person failed to notify their prospective or current firm in writing of an existing OBA or PST. In some cases, individuals did not understand what constitutes an OBA or PST, or did not satisfy important provisions of the rules (*e.g.*, the requirement for written rather than verbal notice). In other cases, individuals failed to provide the information with sufficient detail for a firm to make an adequate determination as to whether to allow a proposed OBA or PST to proceed.
- **OBA and PST Notice Reviews –** FINRA observed weaknesses in some firms' OBA and PST reviews. In some instances, firms either did not have written supervisory procedures for such reviews or the procedures were inadequate. FINRA also observed instances where firms had well-designed procedures, but executed them poorly, either through a lack of supporting documentation or a failure to execute their reviews with sufficient depth. In particular, some firms construed "compensation" too narrowly, erroneously determined that an activity was not a PST, or approved participation in a proposed transaction without adequately considering whether they could supervise the transaction as if it were executed on their own behalf.
- **Post-PST Approval –** FINRA observed several problems once firms decided to approve PSTs for compensation. Some firms did not fully understand the activity and, as a result, failed to supervise it effectively. Other firms did not retain the documentation necessary to demonstrate their compliance with the supervisory obligations. In addition, firms sometimes had difficulty recording the transactions on their books and records because PSTs can take many forms and the uniqueness of their structures may not fit easily into firm electronic systems that are designed with fields tailored to a firm's existing business.[6] Some firms failed to monitor limitations placed on the PST, such as a prohibition on a registered representative soliciting firm clients to participate in the PST.

Anti-Money Laundering Compliance Program

Following the terrorist attacks of September 11, 2001, Congress passed the USA PATRIOT Act, in part, to strengthen the anti-money laundering (AML) and counter-terrorist financing provisions of the Bank Secrecy Act (BSA) and extend them to broker-dealers. Among other provisions, the BSA requires firms to monitor for, detect and report suspicious activity to the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN).

FINRA Rule 3310 requires that members develop and implement a written AML program reasonably designed to comply with the requirements of the BSA, and the implementing regulations promulgated thereunder by the Department of the Treasury.[7]

FINRA observed that firms with effective AML programs actively tailor their risk-based AML program to the firm's business model and associated AML risks as opposed to simply implementing a more "generic" program. They also conducted independent testing that included sampling customer accounts in order to test whether the firm was collecting and verifying customer identification information on all individuals and entities that would be considered customers under the BSA, as well as trading and money movement activity to test whether the firm was performing adequate monitoring for and investigations of potentially suspicious activity. In addition, they designed training programs that were specific to the roles and responsibilities of the participating employees and captured current and evolving aspects of the AML landscape.

Selected Examination Findings

FINRA observed instances where firms failed to establish and implement an AML program reasonably designed to detect, and cause the reporting of, suspicious activity.

- **Maintaining Adequate Policies and Procedures for Suspicious Activity –** Some firms failed to establish and implement risk-based policies and procedures to detect and report suspicious transactions. FINRA identified these deficiencies where, for example, a firm's business growth far outpaced the growth of its AML programs, a portion of a firm's business involved a high-risk product (such as microcap securities or dual currency bonds), or a firm's business evolved over time and AML policies and procedures were not updated and adequately tailored to the firm's current risks, including with respect to how potentially suspicious activity would be monitored and documented.
- **Responsibility for AML Monitoring –** While firms are permitted to delegate aspects of their suspicious activity monitoring program to non-AML staff (*e.g.*, to business line staff responsible for trade surveillance), in some cases where this was done, FINRA observed that problems sometimes arose with the appropriate and adequate escalation of potentially suspicious activity. Those problems typically occurred when the AML and surveillance staff did not share a common understanding of the types of activities that merited escalation or when staff did not escalate such activities appropriately. In some cases, the problems occurred because firms did not: (1) clearly define the activities that were being delegated; (2) articulate those delegations and related surveillance responsibilities in their written supervisory procedures; or (3) adequately train non-AML staff on AML surveillance policies and procedures.
- **Exclusions From Data Feeds Used for AML Monitoring –** FINRA also observed instances where firms' monitoring systems were deficient due to gaps in the data feeding those systems that were created, for example, by the use of "suspense accounts" to process foreign currency money movement and conversion. The use of suspense and other operational accounts sometimes obscured the source of funds to firms' surveillance systems, resulting in weaker monitoring of high-risk transactions. FINRA also observed instances where firms made decisions to exclude certain types of customer accounts from monitoring programs, but failed to document or, if circumstances changed, revisit the risk-based rationale for the decision, again resulting in unidentified suspicious activity.

- **Resources for AML Monitoring –** FINRA also identified deficiencies due to policies and procedures not being implemented as a result of firms not providing adequate resources to AML departments to carry out the responsibilities of the AML program. This result was more common when a firm experienced significant growth but did not grow the firm's AML program commensurately. The lack of resources can lead to deficient monitoring or inadequate investigations of potentially suspicious activity.
- **Independent Testing of AML Monitoring –** FINRA also observed that some firms did not ensure the independent testing required under FINRA Rule 3310(c) included a review of how the firm's AML program was implemented. Other weaknesses included firms not ensuring the independence of the test, or not completing tests on an annual calendar year basis where the firm's business warranted that regular testing.

Product Suitability

FINRA Rule 2111 states that a "member or an associated person must have a reasonable basis to believe that a recommended transaction or investment strategy involving a security or securities is suitable for the customer, based on the information obtained through the reasonable diligence of the member or associated person to ascertain the customer's investment profile." In addition, FINRA Rule 3110 obligates firms to establish and maintain a system to supervise the activities of associated persons that is reasonably designed to achieve compliance with applicable securities laws and regulations and FINRA rules.

The concerns that FINRA had during the course of examinations with regard to the suitability of certain products and their supervision did not vary materially by firm size, but did occur more frequently in connection with certain product classes, specifically unit investment trusts (UITs) and certain multi-share class and complex products, such as leveraged and inverse exchange-traded funds (ETFs). FINRA observed firms that implemented a variety of effective practices in recommending the purchase or sale of these products, which included thoroughly training registered representatives on products' performance and risk characteristics, as well as establishing criteria to consider in determining whether a product was suitable for a specific customer; communicating product risks to customers in a way those customers could understand; and tailoring supervisory systems to products' features and sources of risk to customers. For example, with respect to UITs, FINRA observed firms that alerted customers to the consequences of selling and reinvesting in a new UIT prior to the initial UIT's maturity using negative or positive consent letters. Some firms implemented surveillance patterns to identify early UIT rollovers under a variety of scenarios. In addition, some firms required registered representatives to enter a rationale into firm systems for each short-term UIT transaction and coupled the entry with documented supervisory review.

Selected Examination Findings

- **UITs**

  UITs are generally structured portfolios with maturities aligned to meet the objective of the strategy. Typically, the vast majority of UITs purchased are not traded or redeemed significantly in advance of maturity without a customer-specific need for liquidation or specific changes in the economic environment. Given that registered representatives earn most of the fees associated with UITs at or shortly following the initial offering period, there is a risk that they may recommend early rollovers or exchanges to increase their sales credits.

  FINRA identified instances in which customers were advised to roll their UIT investments over early, and firms did not have appropriate supervisory mechanisms in place to identify and review the suitability of the recommendation.[8] This practice causes investors to incur additional sales charges, including both creation and development fees and deferred sales charges.

Some firms FINRA reviewed failed to adequately identify short-term UIT trading activity as an area of potential abuse by registered representatives, and did not implement adequate internal controls to identify potentially problematic UIT trading activity. For example, some firms' systems and processes looked at individual short-term UIT trades in isolation, but did not have processes to capture patterns of short-term UIT trades across customer accounts, registered representatives, branch office location, or to look for patterns of series-to-series UIT trading, excessive early liquidations followed by subsequent purchases, or cross-product trading partially involving UITs.

FINRA observed that the quality of a firm's supervision for potentially problematic short-term trading of UITs was often correlated with the degree of specificity in a firm's definition of such trading. Some firms defined a UIT short-term trade to include multiple scenarios (*e.g.*, rollovers, early rollovers, exchanges, series-to-series transactions prior to an approaching maturity). By contrast, other firms had more limited definitions (*e.g.*, excluding early rollovers). This more limited definition reduced the efficacy of the firm's supervision and surveillance.

► Multi-Share Class and Complex Products

FINRA found that some firms failed to meet their suitability obligations with respect to individual customers when recommending multi-share class or complex products. For example, FINRA observed situations where firms: (1) recommended a higher-fee share class without a reasonable basis to believe that the recommendation was suitable; or (2) recommended a complex product without a reasonable basis to believe the product was suitable in light of the customer's risk tolerance and investment time horizon. In some instances, firms also failed to seek to obtain key pieces of investor profile information, without providing a reasonable basis for failing to do so.

In addition, FINRA observed that some firms failed to establish and implement adequate supervisory systems and written supervisory procedures with regard to multi-share class and complex products. At one firm, for example, FINRA observed that in a sample of short-term surrender variable annuity transactions, over 50 percent of customers had a long-term investment time horizon. Despite this appearance of a conflict with the recommendation to purchase the short-term surrender annuity, FINRA found no evidence in most of the transactions that the firm had performed a supervisory review addressing these concerns. At other firms, FINRA found that the suitability of recommendations for the purchase of leveraged or inverse ETFs had not been subject to adequate supervisory reviews.[9]

► Training

Some firms failed to provide adequate training for registered representatives with respect to suitability issues, particularly regarding the products described above. Consequently, they were neither sufficiently knowledgeable to make customer-specific suitability determinations nor to advise customers effectively on the risks those products entailed. In the case of UITs, for example, firms that relied on written supervisory procedures and compliance bulletins to inform their registered representatives and principals about UITs encountered more sales practice problems than firms that implemented UIT-focused training for registered representatives.

Best Execution

Best execution is a significant investor protection requirement that essentially obligates a broker-dealer to exercise reasonable care to execute a customer's order in a way to obtain the most advantageous terms for the customer. As the circumstances of each order and trading environment vary, so does the determination of what is best execution. Broker-dealers must be cognizant of the duty of best execution they owe customers when they receive, handle, route or execute customer orders in equities, options and debt securities. If a broker-dealer receives an order-routing inducement, such as payment for order flow, or trades as principal with customer orders, it must not let those factors interfere with its duty of best execution nor take them into account in analyzing market quality.

Generally, FINRA Rule 5310 requires that in any transaction for or with a customer or a customer of another broker-dealer, a member and persons associated with a member, shall use reasonable diligence to ascertain the best market for the subject security, and buy or sell in such market so that the resultant price to the customer is as favorable as possible under prevailing market conditions.

In lieu of an order-by-order review, the rule permits firms that route customer orders to other broker-dealers for execution on an automated, non-discretionary basis, as well as firms that internalize customer order flow, to conduct a periodic (at least quarterly) regular and rigorous review of execution quality likely to be obtained from different market centers.[10]

FINRA observed firms that established, maintained, and enforced policy and supervisory procedures regarding regular and rigorous reviews for execution quality, including a description of the reviews performed and how the conduct and results of the reviews should be documented. Those firms documented their conduct of such reviews, the data and other information considered, order routing decisions and the rationale used. This is important not only to allow firms to make appropriate routing decisions, but also so that a regulator will understand what information was considered and why.

Selected Examination Findings

FINRA had concerns regarding the duty of best execution at firms of all sizes that receive, handle, route or execute customer orders in equities, options and fixed income securities.[11] FINRA found that some firms failed to implement and conduct an adequate regular and rigorous review of the quality of the executions of their customers' orders. These deficiencies included:

- failing to compare the quality of the executions firms obtained via their order routing and execution arrangements (including the internalization of order flow) against the quality of the executions they could have obtained from competing markets;
- failing to conduct reviews of certain types of orders (*i.e.*, market, marketable limit and non-marketable limit orders); and
- failing to consider certain factors set forth in FINRA Rule 5310 when conducting a regular and rigorous review, such as speed of execution, price improvement and the likelihood of execution, among others.

As a result of such deficiencies, these firms failed to assure that order flow was directed to markets providing the most beneficial terms for their customers' orders. FINRA notes that conducting a regular and rigorous review of customer execution quality is critical to the supervision of best execution practices, particularly if a firm routes customer orders to an alternative trading system in which the firm has a financial interest or market centers that provide order routing inducements, such as payment for order flow arrangements and order routing rebates.[12]

Market Access Controls

As trading in the U.S. securities markets has become more automated, the potential impact of a trading error or a rapid series of errors—caused by a computer or human error, or a malicious act—has become more severe. The SEC adopted Securities Exchange Act (SEA) Rule 15 c3-5 (referred to as the SEC's "Market Access Rule") to require broker-dealers with market access or that provide market access to their customers to "appropriately control the risks associated with market access so as not to jeopardize their own financial condition, that of other market participants, the integrity of trading on the securities markets, and the stability of the financial system."[13] For such broker-dealers, the Market Access Rule applies to trading in all securities on an exchange or alternative trading system, including equities, options, ETFs, debt securities (including municipals and treasuries) and security-based swaps.

FINRA observed firms that provide market access implement a variety of effective controls to help satisfy the requirements of SEA Rule 15c3-5, such as maintaining reasonable documentation to support thresholds; conducting periodic reviews that assess the reasonableness of thresholds (*e.g.*, through a credit or capital utilization review); aggregating capital or credit usage limits by assigning finely tuned or granular limits, which in total represent a reasonable threshold, or by aggregating across applicable measures (*e.g.*, accounts and systems) on a pre-trade basis; and establishing well-defined procedures that clearly describe the process to adjust a threshold both on an intra-day and permanent basis.[14]

Selected Examination Findings

FINRA observed several areas where some firms that provide market access fall short of their obligations under SEA Rule 15c3-5, particularly with respect to the establishment of pre-trade financial thresholds, implementing and monitoring aggregate capital or credit exposures, and tailoring erroneous trade controls.

FINRA also found that some firms did not appropriately apply the Market Access Rule to some or all of their fixed income activities. The Market Access Rule applies to any of a firm's fixed income trading activity directed to an alternative trading system or exchange, including from a firm's proprietary and principal trading desks, even if such activity represents a small percentage of the firm's overall fixed income trading activity.[15]

- **Establishing Pre-Trade Financial Thresholds –** FINRA observed instances in which firms failed under the Market Access Rule to establish reasonable pre-trade financial thresholds (capital and credit), or to undertake reasonable due diligence to substantiate those firm-assigned thresholds. For example, in one examination, FINRA noted that a firm assigned unreasonably high financial thresholds to its broker-dealer affiliate and was unable to provide any empirical data to support those thresholds. Certain single-trader IDs within the affiliate were assigned buying power of hundreds of millions of dollars and had a combined buying power of several billion dollars. The firm also lacked any substantiation of the reasonableness of those thresholds.
- **Implementing and Monitoring Aggregate Financial Exposures –** FINRA observed instances where firms did not adequately consider capital and credit usage in the aggregate.[16] FINRA also observed instances where firms providing market access lacked procedures on how to request, review, or approve adjustments to capital or credit thresholds. Often such adjustments were made on an *ad hoc* basis (*e.g.*, in expectation of increased order flow in response to a market event, such as an index rebalancing) and not sufficiently documented. In some cases, the firm did not reset the adjusted levels or maintain documentation to support a permanent increase in the capital or credit threshold.

- **Tailoring Erroneous or Duplicative Order Controls –** Striking a reasonable balance between preventing potentially erroneous or duplicative orders while not unduly inhibiting trading can be challenging. FINRA observed instances in which firms did not appropriately tailor their erroneous or duplicative order controls to particular products, situations or order types. For instance, firms use an "away from the market" control to prevent erroneous orders.[17] However, relying solely on this control may put a firm at risk when entering large market orders, as there is no limit order price reference point. An effective practice that FINRA has observed to reasonably prevent erroneous orders of this type is to employ a market impact check, which measures the size of a customer's order compared to the average daily volume in that security. If a check of this type is used, it should be set at a reasonable level.[18]

  FINRA also observed situations where a firm had not considered the character of the market at the time of order entry. For instance, firms that only used the "away from the market" control may have created issues at times when the NBBO may not have been indicative of the true market.[19] When the NBBO spread is above a preset percentage, FINRA has observed that one effective practice to prevent erroneous orders is for the firm to establish an alternative reference point, such as a control that measures the order price as a percentage away from last sale as opposed to the NBBO.

- **Implementing Effective Fixed Income Financial Controls –** FINRA observed that in some instances, firms were not implementing the required systemic pre-trade "hard" blocks to prevent fixed income orders from reaching an alternative trading system that would cause the breach of a threshold. These firms implemented either "soft" blocks that provided warnings, but did not stop (automatically or manually) orders in breach of a threshold from being executed, or post-execution controls. One firm's systems permitted a customer to enter an additional order that breached the customers' credit thresholds before imposing the hard block. In some cases, firms that initially implemented controls to address the rule's requirements failed to establish market access controls as they added new alternative trading systems.
- **Reliance on Vendors for Fixed Income Financial Controls –** Firms may rely on an outside vendor's tools, including those of an alternative trading system, to effect their financial controls, but they must have direct and exclusive control over the mechanisms that have been established and remain responsible for compliance. However, FINRA observed some firms that allowed the alternative trading system to set capital thresholds for their fixed income orders instead of establishing their own thresholds. Occasionally, firms were not sure what their thresholds were, and had no means to monitor their usage during the trading day. Some firms failed to understand how their vendors' controls worked and could not explain them to FINRA.
- **Effective Testing for Fixed Income Financial Controls –** Firms also must periodically test their market access controls, which forms the basis for an annual CEO certification attesting to a firm's controls. FINRA found that in some instances, firms either failed to conduct any tests at all for their fixed income orders, or relied on their vendors to perform the tests without appropriate due diligence by the firm.

Summary of Additional Observations

In addition to the topics we address above, FINRA also draws firms' attention to the following areas where operational deficiencies have challenged some firms' ability to meet their compliance obligations.

Alternative Investments Held in Individual Retirement Accounts (IRAs)

FINRA has identified instances in which firms that carry customers' alternative investment assets held in IRAs failed to apply the requirements of financial and operational rules applicable to those assets.[20]

- **Failure to Establish Possession or Control as Required by SEA Rule 15c3-3 (referred to as the SEC's "Customer Protection Rule") –** In some instances, firms that maintained custody of customers' alternative investment assets held in IRAs did not satisfy the requirements for establishing possession or control as per the SEC's Customer Protection Rule and the interpretations thereunder. This problem was observed in instances when firms sold alternative investment assets to customers through their own platform, and also when firms accommodated customers and provided custody for such assets that customers obtained elsewhere, but erroneously concluded they had not taken on custodial responsibilities.
- **Incorrect Account Statements –** FINRA also observed instances where a firm maintained custody of customers' alternative investment assets held in IRAs, but incorrectly reflected customer positions on the customer account statements as assets that were not in the custody of the firm.
- **Inaccurate Net Capital and Reserve Formula Computations –** Some firms prepared inaccurate net capital and reserve formula computations pursuant to SEC rules with respect to alternative investment assets they carried. This issue occurred when firms failed to perform required quarterly verifications of customers' alternative investment account positions and consequently could not factor reconciliation differences into those calculations.

Net Capital and Credit Risk Assessments

FINRA observed that, in seeking to comply with SEA Rule 15c3-1 (referred to as the SEC's "Net Capital Rule") and the interpretations thereunder, some firms faced challenges assessing the creditworthiness of non-convertible debt or money market instruments they held in their inventory for client facilitation or other purposes. These challenges increased following the effective date for compliance with amendments to SEC rules that removed references to credit ratings in order to reduce reliance on credit rating agencies and help ensure that haircut charges for certain securities for purposes of net capital computations are consistent with market data.[21] FINRA observed issues principally in six areas:

- **Inadequate Policies and Procedures –** In some instances, firms did not adequately design or document their policies and procedures for assessing and monitoring creditworthiness.
- **Inappropriate Use of Thresholds for Conducting Assessments to Determine if Securities Have Minimal Credit Risk –** Pursuant to the SEC rule, firms are permitted to apply either a 15 percent haircut to all of their preferred stock, debt securities and money market instruments that have a ready market, or a lower haircut on such securities if it is determined that they have minimal credit risk pursuant to policies and procedures as specified under the Net Capital Rule. FINRA has noted instances where firms first applied the lower haircut to all such securities and then used a threshold to determine for which of those securities they would perform an analysis to determine minimal credit risk. However, the rule makes no allowance for a *de minimis* threshold below which the required creditworthiness assessment need not be performed.

- **Misapplication of SEC No-Action Letters –** FINRA noted instances where firms incorrectly applied the criteria in SEC no-action letters for determining whether a security may be deemed to have a "ready market" to certain securities that are not within the scope of those letters. In particular, FINRA noted instances where firms incorrectly applied guidance for high-yield bonds to asset-backed securities held in their inventory. In other instances, firms did not properly apply the haircut charges prescribed in the no-action letters, and as a result applied lower haircut charges not consistent with the SEC staff's guidance.
- **Failure to Apply Proper Charges for Open Contractual Commitments –** FINRA noted instances where firms applied lower haircut charges to their open contractual commitments without performing the required assessment of creditworthiness as required by SEA Rule 15c3-1(c)(2)(vi)(I).
- **Improper Use of Indices as Benchmarks for Credit Risk Assessments –** Some firms incorporated indices or other data into their procedures as benchmarks to assess the credit worthiness of an instrument, but did not reasonably design their use of such benchmarks to be consistent with the Net Capital Rule. For example, some firm procedures used certain benchmarks, but then did not articulate the levels at which the benchmarks would indicate a minimal amount of credit risk.
- **Inappropriate Use of Internal or External Credit Risk Assessments –** Firms may incorporate credit ratings developed by an affiliate into their own procedures for assessing creditworthiness, but SEC rules require that procedures informed by such ratings must still be reasonably designed to result in assessments of creditworthiness that typically are consistent with market data. FINRA observed some instances where the use of an affiliate's credit ratings did not support such procedures, such as one instance where the ratings used in the procedures were not kept current.

Order Capacity

FINRA observed that firms of all sizes that engage in an equities business sometimes failed to comply with the requirement to enter the correct capacity code (*e.g.*, agency, principal, riskless-principal) when reporting an off-exchange trade to a FINRA equity trade reporting facility.[22]

Specifically, FINRA observed firms that failed to reasonably address requirements in the development and programming of record keeping and order entry systems, maintain written supervisory procedures reasonably designed to achieve compliance with trade reporting rules, adequately train employees with respect to the significance of properly marking capacity in order entry systems, and adequately supervise employees with respect to the proper marking. These failures resulted in, among other issues, deficiencies in the proper marking and reporting of numerous orders or executions by firms' proprietary or vendor-provided systems.

In the case of equity reporting to a FINRA facility, FINRA continued to identify firms that incorrectly reported riskless principal transactions as agent, or agency transactions as riskless principal transactions. These errors reflected some firms' misunderstanding of the key distinction between agency and riskless principal transactions: the former do not traverse through the firm's principal accounts, unlike principal and riskless principal transactions.

Regulation SHO

FINRA observed some instances in which firms have had difficulty meeting various aspects of their obligations under Regulation SHO and relevant FINRA rules:

- **Supervision of Third-Party Order Management Systems –** FINRA found that some firms may be overly reliant upon a third-party order management system for supervisory and compliance functions. FINRA noted inadequate levels of firm review and verification that third-party systems properly accounted for open sell orders as required by FAQ 2.5 concerning Regulation SHO and properly marked orders in accordance with Rule 200(g) of Regulation SHO.
- **Trading Records From Third-Party Order Management Systems –** Some firms were hindered from adequately conducting these supervisory reviews as a result of limitations with vendor-provided information and data and vendor non-responsiveness. FINRA found that some third-party vendors did not provide firms with trading records that would permit a review of order marking for compliance with Rule 200(g) of Regulation SHO and FAQ 2.5. Specific limitations that FINRA identified included: (1) firms that were unable to obtain trading records that provided proprietary order information (as opposed to trade execution information); (2) vendors that did not have a single report that captured proprietary order information; and (3) vendors that did not provide trading data in a format that firms could use to conduct testing and review for order marking (*e.g.*, PDF documents that could not be converted to a more easily useable format).
- **Locate Obligations –** FINRA observed weaknesses in various aspects of certain firms' locate practices. In some cases, firms continued to provide locates after depleting available shares, while in others there were weaknesses in some firms' processes to document manual locates after available shares were depleted. FINRA also found that firms failed to establish proper controls to ensure that "easy to borrow" lists were accurate and updated timely to reflect current market or other conditions, such as existing fails to deliver or securities designated "hard to borrow."
- **Fail-to-Deliver Closeouts –** FINRA observed instances where firms did not maintain adequate written supervisory procedures for complying with Rule 204 of Regulation SHO regarding closeout of fails to deliver. The procedures did not address, for example, actions to be taken when transactions in American Depository Receipts did not settle on the applicable settlement date or how firms would ensure their books and records are net flat or net long on a day when a closeout obligation existed.

TRACE Reporting

FINRA observed some firms that engaged in institutional sales of fixed income securities frequently did not comply with certain key TRACE reporting rules—FINRA Rules 6730(a)(7),[23] 6730(b)(1) and (2),[24] and 6730(c)(8).[25] Specifically, FINRA found that some firms:

- failed to report transactions in some TRACE-eligible securities because they relied on the master list of TRACE-eligible securities published by FINRA, and did not have a system or process to determine if a transaction involved a security that was not set up in TRACE at the time of the transaction;
- reported transactions to TRACE late—more than 15 minutes from the time of execution—and inaccurately, providing the execution time as the time the transaction was entered into the firm's order management system, not the actual time of execution; and
- failed to detect deficiencies such as those described above, in part because they failed to establish and maintain a supervisory system reasonably designed to achieve compliance with certain TRACE reporting obligations.

Endnotes

1. For additional information on cybersecurity, including FINRA's Small Firm Checklist, please *see* FINRA's cybersecurity topic page.

2. "Spearphishing" is an email attack that typically targets an individual or set of individuals with emails that appear to be from an entity or person known to the target.

3. Some of these observations are more relevant to large firms or firms with a highly technology-dependent business model.

4. A "privileged user" is typically a systems, server, network or a database administrator with unrestricted access to powerful commands that enable him or her to create other users, assign access rights, create, copy, delete, and modify any files and databases, build new servers in production or shut down servers and systems. Often these users are assigned to a technology infrastructure department and support numerous business lines and systems across the whole organization.

5. On May 15, FINRA published *Regulatory Notice 17-20* announcing that FINRA is conducting a retrospective review of the OBA and PST rules and requesting public comment on them. That request was made in the context of FINRA's ongoing effort to review "significant rules to ensure they remain effective at protecting investors in an efficient manner."

6. NASD *Notice to Members 96-33* notes that a firm is "not required to record the activity in the same manner it records transactions executed on behalf of its own firm (*i.e.*, on its purchase and sales blotter). Rather, members may develop and use alternative approaches that meet their specific needs and business practices ..."

7. FINRA provides a free template for small firms to assist them in fulfilling their responsibilities to establish the AML compliance program required by the BSA, its implementing regulations, and FINRA Rule 3310. The template provides text examples, instructions, relevant rules and links to other resources that are useful in developing an AML plan for small firms.

8. FINRA bases its observations here on findings from our cycle examination program as well as a sweep FINRA conducted. The information request for the sweep can be found here.

9. Most recently, FINRA reminded firms of sales practice obligations for volatility-linked exchange-traded products in *Regulatory Notice 17-32*.

10. FINRA has noted in recent guidance that it believes order-by-order review of execution quality is increasingly possible for a range of orders in all equity securities and standardized options. *See Regulatory Notice 15-46*. If a firm chooses not to conduct an order-by-order analysis, a member must determine, based on its regular and rigorous review, whether any material differences in execution quality exist among the markets trading the security and, if so, modify the member's routing arrangements or justify why it is not modifying its routing arrangements.

11. FINRA bases its observations here on findings from our cycle examination program as well as a sweep FINRA conducted. The information request for the sweep can be found here.

12. FINRA recently initiated targeted exams regarding the impact of order routing inducements on a firm's order routing practices and decisions. The information request for the sweep can be found here.

13. Exchange Act Release No. 63241, 75 FR 69792 (Nov. 3, 2010).

14. These procedures included details on the approval process (who has the authority to override or change a threshold) and the steps leading up to that approval. Firms retained clear documentation to support these decisions, and for instances where a limit increase was given on an intra-day basis, procedures that addressed the readjustment of the limit.

15. While the Market Access Rule defines market access as the entry of orders on alternative trading systems and exchanges, with very limited exceptions, nearly all fixed income market access occurs on alternative trading systems.

16. The challenge of considering capital and credit usage in the aggregate generally arose where firms assigned multiple account identifiers or provided services that could create points where thresholds could be multiplied without appropriate monitoring of the aggregate impact. Scenarios that can result in a firm unwittingly multiplying thresholds include those that offer an individual customer multiple trading platforms to route orders to market centers, provide sponsored access or the use of other market center specific controls, establish multiple trading accounts for a single customer, including LLCs (Master/Sub-Accounts), and assign multiple user IDs, monikers or other identifiers to a single customer.

17. An "away from the market" control is a measurement of how far above (buy order) or below (sell order) the National Best Bid and Offer (NBBO) an order is priced. A firm typically assigns a percentage above which an order will be halted.

18. For example, one firm set its control threshold at an unreasonable 500 percent of the average daily volume of the security.

19. The general nature of trading makes the premarket session particularly vulnerable to this scenario. During the premarket, participants' quotes trickle in and the NBBO spread narrows as the regular session opening approaches.

20. "Alternative investments" as used here refers to such products as, among other things, hedge funds, private equity funds, managed future funds, limited partnerships and non-traded Real Estate Investment Trusts (REITs).

21. For more information on the SEC's 2013 credit ratings amendments, please *see* the SEC's Adopting Release.

22. The FINRA/Nasdaq TRF, FINRA/NYSE TRF and OTC Reporting Facility are collectively referred to herein as the "FINRA Facilities."

23. Providing that, if a member makes a good faith determination that a transaction involves a TRACE-eligible security, the member must report the transaction, and if the security is not set up in the TRACE system, the member must promptly contact FINRA prior to reporting the transaction.

24. Requiring that, in a transaction between two members, each member must submit a trade report and, in a transaction between a member and a non-member (including a customer) the member must submit a trade report.

25. Requiring that members report the time of execution of a transaction.

© 2017 FINRA. All rights reserved.
17_0342.1 –11/17

Updated Small Firm Template
[Firm Name]
Anti-Money Laundering (AML) Program:
Compliance and Supervisory Procedures

UPDATED AS OF MONTH DAY, YEAR

This template is provided to assist small firms in fulfilling their responsibilities to establish an Anti-Money Laundering (AML) Program as required by the Bank Secrecy Act (BSA) and its implementing regulations and FINRA Rule 3310 (AML Compliance Program). Nothing in this template creates any new requirements for AML programs. **Furthermore, following this template does not guarantee compliance with AML Program requirements or provide a safe harbor from regulatory responsibility.** There is no exemption from the AML rules for small broker-dealers.

Your firm's AML program should be "risk-based." That means that the program's AML policies, procedures and internal controls should be designed to address the risk of money laundering specific to your firm. Your firm can identify that risk by looking at the type of customers it serves, where its customers are located, and the types of services it offers. It is a good practice to develop a written analysis of your firm's money laundering and terrorist financing risk and how your firm's AML procedures manage that risk. This "risk-assessment" will help to ensure that the AML program is the right one for your firm and is a useful tool for demonstrating to your firm's examiner that the firm used a reasonable approach for designing its AML program.

In addition, where certain AML rules may be inapplicable due to the limited nature of your firm's business, FINRA expects your firm to have internal controls in place to identify when circumstances change in such a way as to trigger previously inapplicable AML requirements and to amend your AML policies and procedures to accurately reflect all AML requirements that are applicable to your business. For example, a firm with no customer accounts within the definition of the Customer Identification Program (CIP) rule would not be expected to have a CIP. However, the firm must have procedures in place to identify when the firm's business activities have shifted in such a way as to require compliance with the CIP rule. In addition, notwithstanding the fact that the firm does not have accounts for CIP purposes, the firm is expected to identify and develop procedures for any additional AML requirements that do apply (*e.g.*, suspicious activity monitoring and reporting).

The language in this template is provided only as a **helpful starting point** to walk you through developing your firm's program. If any of the language does not adequately address your firm's business situation in any respect, you will need to prepare your own

language. **You** are responsible for ensuring that the program fits your firm's risk level and that you implement the program.

TEXT EXAMPLES are provided to give you sample language that you can modify, as necessary, to fit your firm's needs in creating your firm's program.

Material in *italics* provides instructions and citations to the relevant rules, and other resources that you can use to develop your firm's program.

The FINRA AML web page includes important information and links to other websites with useful information. You should also consult the websites maintained by the Financial Crimes Enforcement Network (FinCEN) and the Securities and Exchange Commission (SEC), including the SEC's AML Source Tool and Spotlight on AML Rulemaking for additional information and guidance. For historical guidance and background, you may wish to consult NASD Notices to Members (NTM) 02-21, 02-47, 02-50, 02-78, 02-80, 03-34, 06-07, 06-41 and 07-17. Regulatory Notices 07-42, 08-66, 09-05, 12-08 and 17-40 provide additional guidance information about firms' AML obligations. In addition, FinCEN has a mechanism in place by which firms can electronically fulfill their BSA reporting requirements (BSA E-Filing System). We strongly encourage firms to use the BSA E-Filing System.

1. Firm Policy

TEXT EXAMPLE: It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Bank Secrecy Act (BSA) and its implementing regulations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is 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 further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Although cash is rarely deposited into securities accounts, the securities industry is unique in that it can be used to launder funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Examples of types of

fraudulent activities include insider trading, market manipulation, ponzi schemes, cybercrime and other investment-related fraudulent activity.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable BSA regulations and FINRA rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310.

2. AML Compliance Person Designation and Duties

Designate your firm's AML Compliance Person and describe his or her duties.

TEXT EXAMPLE: The firm has designated [*Name*] as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm's AML program. [*Name*] has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training, including [*describe*]. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees, and [*add any other duties your firm will assign to the AML Compliance Person; review NASD Rules 1021 and 1031[1] for any applicable registration requirements*]. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports (SAR-SFs) are filed with the Financial Crimes Enforcement Network (FinCEN) when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

The firm will provide FINRA with contact information for the AML Compliance Person through the FINRA Contact System (FCS), including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile (if any). The firm will promptly notify FINRA of any change in this information through FCS and will review, and if necessary update, this information within 17 business days after the end of each

[1] As of October 1, 2018, NASD Rules 1021 and 1031 will no longer be effective. As of October 1, 2018, *see* FINRA Rule 1210.

calendar year. The annual review of FCS information will be conducted by [*Name*] and will be completed with all necessary updates being provided no later than 17 business days following the end of each calendar year. In addition, if there is any change to the information, [*Name*] will update the information promptly, but in any event not later than 30 days following the change.

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310; FINRA Rule 4517.
Resources: Regulatory Notice 07-42; NTM 06-07; NTM 02-78. Firms can submit their AML Compliance Person information through FINRA's FCS web page.

3. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

a. FinCEN Requests Under USA PATRIOT Act Section 314(a)

Pursuant to the BSA and its implementing regulations, financial institutions are required to make certain searches of their records upon receiving an information request from FinCEN. Describe your firm's procedures for FinCEN requests for information on money laundering or terrorist activity.

In order for a firm to obtain information requests from FinCEN, the firm must first designate an AML Contact Person in FCS. You should be aware that if you want to change the person who receives FinCEN requests, you must change the AML contact information in FCS. When you are faced with a change in personnel who will receive this information, you should be aware that FinCEN receives a data feed of this revised information from FCS every other week and that it may take several weeks for a firm's new AML contact person to receive information from FinCEN. Therefore, it is advisable for a firm that is aware that a person who had been receiving FinCEN requests is leaving the firm to change the information on FCS as soon as practical to ensure continuity of receiving FinCEN information.

TEXT EXAMPLE: We will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts and transactions (a 314(a) Request) by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in the 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure website. We understand that we have 14 days (unless otherwise specified by FinCEN) from the transmission date of the request to respond to a 314(a) Request. We will designate through the FINRA Contact System (FCS) one or more persons to be the point of contact (POC) for 314(a) Requests and will promptly update the POC information following any change in such information. (*See also* Section 2 above regarding updating of contact information for the AML Compliance Person.) Unless otherwise stated in the 314(a) Request or specified by FinCEN, we are required to search those documents outlined in FinCEN's FAQ. If we find a match, [*Name*] will report it to FinCEN via FinCEN's Web-based 314(a) Secure Information Sharing System

within 14 days or within the time requested by FinCEN in the request. If the search parameters differ from those mentioned above (for example, if FinCEN limits the search to a geographic location), [*Name*] will structure our search accordingly.

If [*Name*] searches our records and does not find a matching account or transaction, then [*Name*] will not reply to the 314(a) Request. We will maintain documentation that we have performed the required search by [*add the details on how your firm will document its searches here. For example, printing a search self-verification document from FinCEN's 314(a) Secure Information Sharing System confirming that your firm has searched the 314(a) subject information against your records OR maintaining a log showing the date of the request, the number of accounts searched, the name of the individual conducting the search and a notation of whether or not a match was found*].

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. [*Name*] will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act with regard to the protection of customers' nonpublic information.

We will direct any questions we have about the 314(a) Request to the requesting federal law enforcement agency as designated in the request.

Unless otherwise stated in the 314(a) Request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the periodic 314(a) Requests as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

Rule: 31 C.F.R. § 1010.520.
Resources: FinCEN's 314(a) web page; NTM 02-80;. FinCEN also provides financial institutions with General Instructions and Frequently Asked Questions relating to 314(a) requests through the 314(a) Secured Information Sharing System or by contacting FinCEN's Regulatory Helpline at (800) 949-2732 or via email at sys314a@fincen.gov.

b. National Security Letters

National Security Letters (NSLs) are written investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) and other federal government authorities conducting counterintelligence and counterterrorism investigations to obtain, among other things, financial records of broker-dealers. ***NSLs are highly confidential. No broker-dealer, officer, employee or agent of the broker-dealer can disclose to any person that a government authority or the FBI has sought or obtained access to records. Firms that receive NSLs must have policies and procedures in place for processing and maintaining the confidentiality of NSLs.*** *If you file a Suspicious Activity Report (SAR-SF) after receiving a NSL, the SAR-SF should not contain any reference to the receipt or existence of the NSL.*

TEXT EXAMPLE: We understand that the receipt of a National Security Letter (NSL) is highly confidential. We understand that none of our officers, employees or agents may directly or indirectly disclose to any person that the FBI or other federal government authority has sought or obtained access to any of our records. To maintain the confidentiality of any NSL we receive, we will process and maintain the NSL by [*describe procedure*]. If we file a SAR-SF after receiving an NSL, the SAR-SF will not contain any reference to the receipt or existence of the NSL. The SAR-SF will only contain detailed information about the facts and circumstances of the detected suspicious activity.

Resource: FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 8 (National Security Letters and Suspicious Activity Reporting) (4/2005).

c. Grand Jury Subpoenas

Grand juries may issue subpoenas as part of their investigative proceedings. The receipt of a grand jury subpoena does not in itself require the filing of a Suspicious Activity Report (SAR-SF). However, broker-dealers should conduct a risk assessment of the customer who is the subject of the grand jury subpoena, as well as review the customer's account activity. If suspicious activity is uncovered during this review, broker-dealers should consider elevating the risk profile of the customer and file a SAR-SF in accordance with the SAR-SF filing requirements. Grand jury proceedings are confidential, and a broker-dealer that receives a subpoena is prohibited from directly or indirectly notifying the person who is the subject of the investigation about the existence of the grand jury subpoena, its contents or the information used to reply to it. If you file a SAR-SF after receiving a grand jury subpoena, the SAR-SF should not contain any reference to the receipt or existence of it. The SAR-SF should provide detailed information about the facts and circumstances of the detected suspicious activity.

TEXT EXAMPLE: We understand that the receipt of a grand jury subpoena concerning a customer does not in itself require that we file a Suspicious Activity Report (SAR-SF). When we receive a grand jury subpoena, we will conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity. If we uncover suspicious activity during our risk assessment and review, we will elevate that customer's risk assessment and file a SAR-SF in accordance with the SAR-SF filing requirements. We understand that none of our officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents or the information we used to respond to it. To maintain the confidentiality of any grand jury subpoena we receive, we will process and maintain the subpoena by [*describe procedure*]. If we file a SAR-SF after receiving a grand jury subpoena, the SAR-SF will not contain any reference to the receipt or existence of the subpoena. The SAR-SF will only contain detailed information about the facts and circumstances of the detected suspicious activity.

Resources: FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 10 (Grand Jury Subpoenas and Suspicious Activity Reporting) (5/2006).

d. Voluntary Information Sharing With Other Financial Institutions Under USA PATRIOT Act Section 314(b)

BSA regulations permit financial institutions to share information with other financial institutions under the protection of a safe harbor if certain procedures are followed. If your firm shares or plans to share information with other financial institutions, describe your firm's procedures for such sharing.

TEXT EXAMPLE: We will share information with other financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. [*Name*] will ensure that the firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. We will use the notice form found at FinCEN's website. Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. We understand that this requirement applies even to financial institutions *with which we are affiliated*, and that we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for example, by segregating it from the firm's other books and records and [*describe any other procedures*].

We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist activities;
- determining whether to establish or maintain an account, or to engage in a transaction; or
- assisting the financial institution in complying with performing such activities.

Rules: 31 C.F.R. § 1010.540.
Resources: FinCEN Financial Institution Notification Form; FIN-2009-G002: Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act (6/16/2009).

e. Joint Filing of SARs by Broker-Dealers and Other Financial Institutions

The obligation to identify and properly report a suspicious transaction and to timely file a SAR-SF rests separately with each broker-dealer. However, one SAR-SF may be filed for a suspicious activity by all broker-dealers involved in a transaction (so long as the report filed contains all relevant and required information) if the SAR-SF is jointly filed. In addition, if a broker-dealer and another financial institution that is subject to the SAR regulations are involved in the same suspicious transaction, the financial institution may also file a SAR jointly (so long as the report filed contains all relevant and required information). For example, a broker-dealer and an insurance company may file one SAR with respect to suspicious activity involving the sale of variable insurance products. Disclosures that are made for the purposes of jointly filing a SAR are protected by the safe harbor contained in the SAR regulations. The financial institutions that jointly file a SAR shall each be separately responsible for maintaining a copy of the SAR and should maintain their own SAR supporting documentation in accordance with BSA recordkeeping requirements. See generally Section 12 (Suspicious Transaction and BSA Reporting) for information on a broker-dealer's obligation to file a SAR to report suspicious transactions.

TEXT EXAMPLE: We will file joint SARs in the following circumstances, according to [*describe procedures*]. We will also share information about a particular suspicious transaction with any broker-dealer, as appropriate, involved in that particular transaction for purposes of determining whether we will file jointly a SAR-SF.

[***If an introducing firm**:*] We will share information about particular suspicious transactions with our clearing broker for purposes of determining whether we and our clearing broker will file jointly a SAR-SF. In cases in which we file a joint SAR-SF for a transaction that has been handled both by us and by the clearing broker, we may share with the clearing broker a copy of the filed SAR-SF.

If we determine it is appropriate to jointly file a SAR-SF, we understand that we cannot disclose that we have filed a SAR-SF to any financial institution except the financial institution that is filing jointly. If we determine it is not appropriate to file jointly (*e.g.*, because the SAR-SF concerns the other broker-dealer or one of its employees), we understand that we cannot disclose that we have filed a SAR-SF to any other financial institution or insurance company.

Rules: 31 C.F.R. § 1023.320; 31 C.F.R. § 1010.430; 31 C.F.R. § 1010.540.

f. Sharing SAR-SFs With Parent Companies

On January 20, 2006, FinCEN issued guidance permitting under certain conditions the sharing of SAR-SFs with either foreign or domestic parent entities.

TEXT EXAMPLE: Because we are a subsidiary, we may share SAR-SFs with [*Name of parent entity (or parent entities)*]. Before we share SAR-SFs with [*Name(s)*], we will have in place written confidentiality agreements or written arrangements that [*Name(s)*] protect the confidentiality of the SAR-SFs through appropriate internal controls.

[***If parent company is a non-U.S. entity**:*] The confidentiality agreement will state that the recipient foreign parent entity (or entities) may not disclose further any SAR-SF, or the fact that such report has been filed. The agreement will allow for the foreign parent entity (or entities) to disclose without permission underlying information (that is, information about the customers and transaction(s) reported) that forms the basis for the SAR-SF and that does not explicitly reveal that a SAR-SF was filed and that is not otherwise subject to disclosure restrictions.

Resource: FinCEN Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities (1/20/2006).

4. Checking the Office of Foreign Assets Control Listings

Although not part of the BSA and its implementing regulations, the Office of Foreign Assets Control (OFAC) compliance is often performed in conjunction with AML compliance. OFAC is an office of the U.S. Treasury that administers and enforces economic sanctions and embargoes based on U.S. foreign policy and national security goals that target geographic regions and governments (e.g., Cuba, Sudan and Syria), as well as individuals or entities that could be anywhere (e.g., international narcotics traffickers, foreign terrorists and proliferators of weapons of mass destruction). As part of its enforcement efforts, OFAC publishes a list of Specially Designated Nationals and Blocked Persons (SDN list), which includes names of companies and individuals who are connected with the sanctions targets. U.S. persons are prohibited from dealing with SDNs wherever they are located, and all SDN assets must be blocked. Because OFAC's programs are constantly changing, describe how you will check with OFAC to ensure that your SDN list is current and also that you have complete information regarding the listings of economic sanctions and embargoes enforced by OFAC affecting countries and parties before opening an account and for existing accounts.

TEXT EXAMPLE: Before opening an account, and on an ongoing basis, [*Name*] will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. (*See* the OFAC website for the SDN list and listings of current sanctions and embargoes). Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. *See also* FINRA's OFAC Search Tool that screens names against the SDN list. [*Name*] will

also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and [*he or she*] will document the review.

If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. We will also call the OFAC Hotline at (800) 540-6322 immediately.

Our review will include customer accounts, transactions involving customers (including activity that passes through the firm such as wires) and the review of customer transactions that involve physical security certificates or application-based investments (*e.g.*, mutual funds).

Rules: 31 C.F.R. § 501.603; 31 C.F.R. § 501.604.
Resources: SEC AML Source Tool for Broker-Dealers, Item 12; OFAC Lists web page (including links to the SDN List and lists of sanctioned countries); FINRA's OFAC Search Tool. You can also subscribe to receive updates on the OFAC Subscription web page. See also the following OFAC forms: Report of Blocked Transactions Form; Report of Rejected Transactions Form; Annual Report of Blocked Property Form; and OFAC Guidance Regarding Foreign Assets Control Regulations for the Securities Industry.

5. Customer Identification Program

Firms are required to have and follow reasonable procedures to document and verify the identity of their customers who open new accounts. These procedures must address the types of information the firm will collect from the customer and how it will verify the customer's identity. These procedures must enable the firm to form a reasonable belief that it knows the true identity of its customers. The final rule, which FinCEN and the SEC jointly issued on April 30, 2003, applies to all new accounts opened on or after October 1, 2003.

The firm's customer identification program (CIP) must be in writing and be part of the firm's AML compliance program.

Note that the CIP rule applies only to "customers" who open new "accounts" with a broker-dealer. Specifically, the CIP rule defines a "customer" as (1) a person that opens a new account or (2) an individual who opens a new account for an individual who lacks legal capacity or for an entity that is not a legal person. "Customer" does not refer to persons who fill out account opening paperwork or who provide information necessary to establish an account, if such persons are not the accountholder as well.

Also, for purposes of the CIP rule's definition of customer, the following entities are excluded from the definition of "customer":

- *a financial institution regulated by a federal functional regulator (that is, an institution regulated by the Board of Governors of the Federal Reserve; Federal Deposit Insurance Corporation; National Credit Union Administration; Office of the Comptroller of the Currency; Office of Thrift Supervision; Securities and Exchange Commission; or Commodity Futures Trading Commission) or a bank regulated by a state bank regulator;*
- *a department or agency of the United States, of any State, or of any political subdivision of any State;*
- *any entity established under the laws of the United States, of any State, or of any political subdivision of a State that exercises governmental authority on behalf of the United States, any State, or any political subdivision of a State;*
- *any entity, other than a bank, whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange or whose common stock or analogous equity interests have been designated as a NASDAQ National Market Security listed on the Nasdaq Stock Market (except stock or interests listed under the separate "NASDAQ Capital Markets Companies" heading), provided that, if the person is a financial institution, other than a bank, only to the extent of its domestic operations; or*
- *a person that has an existing account with the broker-dealer, provided the broker-dealer has a reasonable belief that it knows the true identity of the person.*

Accordingly, a broker-dealer is not required to verify the identities of persons with existing accounts at the firm, as long as the broker-dealer has a reasonable belief that it knows the true identity of the customer.

For purposes of the CIP rule, an "account" is defined as a formal relationship with a broker-dealer established to effect transactions in securities, including, but not limited to, the purchase or sale of securities, securities loan and borrowing activity, and the holding of securities or other assets for safekeeping or as collateral. The following are excluded from the definition of "account": (1) an account that the broker-dealer acquires through any acquisition, merger, purchase of assets or assumption of liabilities and (2) an account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974 (ERISA).

Rule: 31 C.F.R. § 1023.220.
Resources: SEC Staff Q&A Regarding the Broker-Dealer Customer Identification Program Rule (October 1, 2003); NTM 03-34; FIN-2006-G007: Frequently Asked Question: Customer Identification Program Responsibilities under the Agency Lending Disclosure Initiative (4/25/2006).

Describe how you will identify customers and verify their identities.

Note that a clearing firm does not have an obligation to perform CIP for an introduced customer if the clearing firm and the introducing firm have entered into a clearing agreement under which the functions of opening and approving customer accounts and directly receiving and accepting orders from the introduced customer are allocated

exclusively to the introducing firm and the functions of extending credit, safeguarding funds and securities, and issuing confirmations and statements are allocated to the clearing firm. This position also extends to piggybacking arrangements[2] where, pursuant to a piggybacking arrangement with an introducing firm, the piggybacking firm retains the functions of opening and approving customer accounts and directly receiving and accepting orders from introduced customers. Thus, under a piggybacking arrangement, the clearing firm and the introducing firm are not obligated to perform CIP for the customers introduced by the piggybacking firm, provided the proper agreement is in place.

Please note that a clearing firm's and introducing firm's AML programs should contain risk-based policies, procedures, and controls for assessing the money laundering risk posed by its fully disclosed clearing arrangements, for monitoring and mitigating that risk, and for detecting and reporting suspicious activity.

Resources: FIN-2008-G002: Customer Identification Program Rule No-Action Position Respecting Broker-Dealers Operating Under Fully Disclosed Clearing Agreements According to Certain Functional Allocations (3/4/2008) and FIN-2008-R008: Bank Secrecy Act Obligations of a U.S. Clearing Broker-Dealer Establishing a Fully Disclosed Clearing Relationship with a Foreign Financial Institution (6/3/2008).

TEXT EXAMPLE:

EITHER:

In addition to the information we must collect under FINRA Rules 2090 (Know Your Customer) and 2111 (Suitability) and the 4510 Series (Books and Records Requirements), and Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts) and 17a-3(a)(17) (Customer Accounts), we have established, documented and maintained a written Customer Identification Program (CIP). We will collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide the required adequate CIP notice to customers that we will seek identification information to verify their identities; and compare customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government. *See* Section 5.g. (Notice to Customers) for additional information.

OR:

[2] In a "piggybacking" arrangement, an introducing firm (the piggybacking firm) does not enter into a clearing agreement with a clearing firm, but rather establishes a relationship with an introducing firm that has established a clearing arrangement with a clearing firm, thus piggybacking off the introducing firm's clearing agreement. FIN-2008-G002 at p.2.

We do not open or maintain customer accounts within the meaning of 31 CFR 1023.100, in that we do not establish formal relationships with "customers" for the purpose of effecting transactions in securities. If in the future the firm elects to open customer accounts or to establish formal relationships with customers for the purpose of effecting transactions in securities, we will first establish, document and ensure the implementation of appropriate CIP procedures. *(Note that a change in the firm's business to accept customer accounts may be a material change in business requiring an application, review and approval by FINRA. See NASD Rule 1017).*

NOTE: ***If your firm deals only with entities that are exempt from the definition of "customer," describe how your firm will confirm and document that the entities are exempt.***

TEXT EXAMPLE: We will collect information to determine whether any entity opening an account would be excluded as a "customer," pursuant to the exceptions outlined in 31 CFR 1023.100(d)(2)) (*e.g.*, documentation of a company's listing information, licensing or registration of a financial institution in the U.S, and status or verification of the authenticity of a government agency or department).

Rule: 31 C.F.R. § 1023.220.
Resources: SEC Staff Q&A Regarding the Broker-Dealer Customer Identification Program Rule (10/1/2003); NTM 03-34.

a. Required Customer Information

Prior to opening an account, [*Name of person or category of associated person*] will collect the following information for all accounts, if applicable, for any person, entity or organization that is opening a new account and whose name is on the account:

(1) the name;
(2) date of birth (for an individual);
(3) an address, which will be a residential or business street address (for an individual), an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office, or other physical location (for a person other than an individual); and
(4) an identification number, which will be a taxpayer identification number (for U.S. persons), or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).

In the event that a customer has applied for, but has not received, a taxpayer identification number, we will *[add procedures describing who, what, when and how]* to confirm that the application was filed before the customer opens the account and to

obtain the taxpayer identification number within a reasonable period of time after the account is opened.

When opening an account for a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

Rule: 31 C.F.R. § 1023.220(a)(2)(i).

b. Customers Who Refuse to Provide Information

Describe your firm's policy for customers who do not provide requested information.

TEXT EXAMPLE: If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Person will be notified so that we can determine whether we should report the situation to FinCEN on a SAR-SF.

c. Verifying Information

Describe how you will verify customers' identities using the information described above. The information you gather may vary according to the risks posed by the type of account. The procedures must enable you to form a reasonable belief that you know the true identity of each customer. Among the risks to consider are the various types of accounts maintained by the firm, the various methods the firm uses to open accounts, the various types of identifying information available, and the firm's size, location and customer base. If you believe that some of these risk factors increase the likelihood that you will need more information to know the true identity of your customers, you should determine what additional identifying information might be necessary for a reasonable belief that you know the true identity of your customer and when such additional information should be obtained.

TEXT EXAMPLE: Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. [*Name*] will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means or both. [*Tailor the sentence to your actual situation.*] We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-

documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and

- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity:

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source *[identify reporting agency, database, etc.]*;

- Checking references with other financial institutions; or

- Obtaining a financial statement.

- [*add other non-documentary methods, if applicable*]

We will use non-documentary methods of verification when:
(1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
(2) the firm is unfamiliar with the documents the customer presents for identification verification;
(3) the customer and firm do not have face-to-face contact; and
(4) there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Person, file a SAR-SF in accordance with applicable laws and regulations.

We recognize that the risk that we may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. We will identify customers that pose a heightened risk of not being properly identified. We will also take the following additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient: [*Add additional procedures for verifying identity of certain customers, such as obtaining information about beneficial ownership, individuals with authority or control over such account. Remember to describe who will take the action, when and how they will obtain the information and what courses of action may be required.*]

Rule: 31 C.F.R. § 1023.220(a)(2)(ii).

d. Lack of Verification

Describe your procedures for responding to circumstances in which the firm cannot form a reasonable belief that it knows the true identity of a customer.

TEXT EXAMPLE: When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (3) close an account after attempts to verify a customer's identity fail; and (4) determine whether it is necessary to file a SAR-SF in accordance with applicable laws and regulations.

Rule: 31 C.F.R. § 1023.220(a)(2)(iii).

e. Recordkeeping

Describe your recordkeeping procedures.

TEXT EXAMPLE: We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep

records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

Rule: 31 C.F.R. § 1023.220(a)(3).

f. Comparison with Government-Provided Lists of Terrorists

Describe how you will check government lists within a reasonable period of time after opening an account (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list). See NTM 02-21, page 6. There currently are no government-provided lists of suspected terrorists that firms are required to use as part of their CIP.

TEXT EXAMPLE: At such time as we receive notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, we will, within a reasonable period of time after an account is opened (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list), determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such by Treasury in consultation with the federal functional regulators. We will follow all federal directives issued in connection with such lists.

We will continue to comply separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

Rule: 31 C.F.R. § 1023.220(a)(4).
Resource: NTM 02-21, page 6, n.24.

g. Notice to Customers

The CIP Rule requires you to provide adequate notice to customers that you are requesting information from them to verify their identities. You may provide such notice by a sign in your lobby, through other oral or written notice, or, for accounts opened online, notice posted on your website. No matter which methods of giving notice you choose, you must give it before an account is opened.

FINRA has produced a Customer Identification Program Notice to assist firms in fulfilling this notification requirement. Please refer to the FINRA AML web page for further details.

TEXT EXAMPLE: We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by federal law. We will use the following method to provide notice to customers: [*describe notice you will provide for each method of account-opening your firm uses (i.e., telephone, online, walk-in, etc.); the final rule provides the following sample language for notice to be provided to a firm's customers, if appropriate:*]

> **Important Information About Procedures for Opening a New Account**
> To help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.
>
> **What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.**

Rule: 31 C.F.R. § 1023.220(a)(5).

h. Reliance on Another Financial Institution for Identity Verification

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our CIP with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

- when such reliance is reasonable under the circumstances;
- when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements of 31 U.S.C. § 5318(h), and is regulated by a federal functional regulator; and
- when the other financial institution has entered into a contract with our firm requiring it to certify annually to us that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program.

[You will not be held responsible for the failure of the other financial institution to fulfill adequately your CIP responsibilities, provided that you can establish that your reliance was reasonable and you have obtained the requisite contracts and certifications.]

Rule: 31 C.F.R. § 1023.220(a)(6).

Resources: No-Action Letters to the Securities Industry and Financial Markets Association (SIFMA) (February 12, 2004; February 10, 2005; July 11, 2006; January 10, 2008; January 11, 2010; January 11, 2011; January 9, 2015; and December 12, 2016)). (The letters provide staff guidance regarding the extent to which a broker-dealer may rely on an investment adviser to conduct the required elements of the CIP rule, prior to such adviser being subject to an AML rule.)

6. Customer Due Diligence Rule

On May 11, 2016, FinCEN adopted a final rule on Customer Due Diligence Requirements for Financial Institutions (CDD Rule) to clarify and strengthen customer due diligence for covered financial institutions, including broker-dealers. The Rule becomes effective on May 11, 2018.

In its CDD Rule, FinCEN identifies four components of customer due diligence: (1) customer identification and verification; (2) beneficial ownership identification and verification; (3) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (4) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. As the first component is already an AML program requirement (under the CIP Rule), the CDD Rule focuses on the other three components.

Specifically, the CDD Rule focuses particularly on the second component by adding a new requirement that covered financial institutions establish and maintain written procedures as part of their AML programs that are reasonably designed to identify and verify the identities of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.

Under the CDD Rule, member firms must obtain from the natural person opening the account on behalf of the legal entity customer, the identity of the beneficial owners of the entity. In addition, that individual must certify, to the best of his or her knowledge, as to the accuracy of the information. FinCEN intends that the legal entity customer identify its ultimate beneficial owner(s) and not "nominees" or "straw men."

The CDD Rule does not prescribe the form in which member firms must collect the required information, which includes the name, date of birth, address and Social Security number or other government identification number of beneficial owners. Rather, member firms may choose to obtain the information by using FinCEN's standard certification form in Appendix A of the CDD Rule (at https://www.fincen.gov/resources/filing-information) or by another means, provided that the chosen method satisfies the identification requirements in the CDD Rule. In any case, the CDD Rule requires that member firms maintain records of the beneficial ownership information they obtain.

Once member firms obtain the required beneficial ownership information, the CDD Rule requires that firms verify the identity of the beneficial owner(s) – in other words, that they are who they say they are – and not their status as beneficial owners through risk-based

procedures that include, at a minimum, the elements required for CIP procedures for verifying the identity of individual customers. Such verification must be completed within a reasonable time after account opening. Member firms may rely on the beneficial ownership information supplied by the individual opening the account, provided that they have no knowledge of facts that would reasonably call into question the reliability of that information.

The CDD Rule's requirements with respect to beneficial owners of legal entity customers applies on a prospective basis, that is, only with respect to legal entity customers that open new accounts from the date of the CDD Rule's implementation. However, member firms should obtain beneficial ownership information for an existing legal entity customer if, during the course of normal monitoring, it receives information that is needed to assess or reevaluate the risk of the customer.

The required records to be created and maintained must include: (i) for identification, any identifying information obtained by the member firm pursuant to the beneficial ownership identification requirements of the CDD Rule, including without limitation the certification (if obtained); and (ii) for verification, a description of any document relied on (noting the type, any identification number, place of issuance and, if any, date of issuance and expiration), of any non-documentary methods and the results of any measures undertaken, and the resolution of each substantive discrepancy. In addition to complying with existing SEC and FINRA record retention requirements, member firms must maintain the records collected as part of the CDD Rule for a minimum of five years after the record is made.

Member firms may rely on the performance by another financial institution (including an affiliate) of the requirements of the CDD Rule with respect to any legal entity customer of the member firm that is opening, or has opened, an account or has established a similar business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions, provided that: (1) such reliance is reasonable under the circumstances; (2) the other financial institution is subject to a rule implementing 31 U.S.C. 5318(h) and is regulated by a Federal functional regulator; and (3) the other financial institution enters into a contract requiring it to certify annually to the member firm that it has implemented its AML program, and that it will perform (or its agent will perform) the specified requirements of the member firm's procedures to comply with the CDD Rule.

The CDD Rule also addresses the third and fourth components, which FinCEN states "are already implicitly required for covered financial institutions to comply with their suspicious activity reporting requirements," by amending the existing AML program rules for covered financial institutions to explicitly require these components to be included in AML programs as a new "fifth pillar." These requirements are discussed further below.

Rules: 31 C.F.R. § 1010.230; 31 C.F.R. § 1023.210(b)(5).

Resources: 81 Fed. Reg. 29398 (May 11, 2016) (Final Rule: Financial Crimes Enforcement Network; Customer Due Diligence Requirements for Financial Institutions); FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (7/19/2016); Regulatory Notice 17-40; FIN-2018-G001: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (4/3/2018).

TEXT EXAMPLE:

EITHER:

In addition to the information collected under the written Customer Identification Program, FINRA Rules 2090 (Know Your Customer) and 2111 (Suitability) and the 4510 Series (Books and Records Requirements), and Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts) and 17a-3(a)(17) (Customer Accounts), we have established, documented and maintained written policies and procedures reasonably designed to identify and verify beneficial owners of legal entity customers and comply with other aspects of the Customer Due Diligence (CDD) Rule. We will collect certain minimum CDD information from beneficial owners of legal entity customers.[3] We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile. We will conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, maintain and update customer information.

OR:

We do not open or maintain accounts for legal entity customers within the meaning of 31 CFR 1010.230. If in the future the firm elects to open accounts for legal entity customers, we will first establish, document and ensure the implementation of appropriate CDD procedures. *(Note that a change in the firm's business to accept accounts for legal entity customers may be a material change in business requiring an application, review and approval by FINRA. See NASD Rule 1017).*

NOTE: ***If your firm deals only with entities that are exempt from the definition of "legal entity customer," describe how your firm will confirm and document that the entities are exempt or excluded.***

a. Identification and Verification of Beneficial Owners

TEXT EXAMPLE

At the time of opening an account for a legal entity customer, [*Name of person or category of associated person*] will identify any individual that is a beneficial owner of the legal entity customer by identifying any individuals who directly or indirectly own 25% or more of the equity interests of the legal entity customer, and any individual with

[3] Beneficial owners and legal entity customers as defined by the CDD Rule.

significant responsibility to control, manage, or direct a legal entity customer. The following information will be collected for each beneficial owner:

(1) the name;
(2) date of birth (for an individual);
(3) an address, which will be a residential or business street address (for an individual), or an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address); and
(4) an identification number, which will be a Social Security number (for U.S. persons), or one or more of the following: a passport number and country of issuance, or other similar identification number, such as an alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).

If your firm elects to utilize Appendix A to 31 CFR § 1010.230, record how the firm will use the document.

For verification, we will describe any document relied on (noting the type, any identification number, place of issuance and, if any, date of issuance and expiration). We will also describe any non-documentary methods and the results of any measures undertaken.

In the event that a beneficial owner of a legal entity customer has applied for, but has not received, a Social Security number (for U.S. persons) or a passport number or other similar identification number (for non-U.S. persons), we will *[add procedures describing who, what, when and how]* to confirm that the application was filed before the customer opens the account and to obtain the applicable identification number within a reasonable period of time after the account is opened.

Rules: 31 C.F.R. § 1010.230(b); 31 C.F.R. § 1023.210(b)(5).
Resources: FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (7/19/2016); Regulatory Notice 17-40.

b. Understanding the Nature and Purpose of Customer Relationships

FinCEN states that the CDD Rule requires that firms must necessarily have an understanding of the nature and purpose of the customer relationship in order to determine whether a transaction is potentially suspicious and, in turn, to fulfill their SAR obligations. To that end, the CDD Rule requires that firms understand the nature and purpose of the customer relationship in order to develop a customer risk profile. The customer risk profile refers to information gathered about a customer to form the baseline against which customer activity is assessed for suspicious transaction reporting. Information relevant to understanding the nature and purpose of the customer relationship may be self-evident and, depending on the facts and circumstances, may

include such information as the type of customer, account or service offered, and the customer's income, net worth, domicile, or principal occupation or business, as well as, in the case of existing customers, the customer's history of activity. The CDD Rule also does not prescribe a particular form of the customer risk profile. Instead, the CDD Rule states that depending on the firm and the nature of its business, a customer risk profile may consist of individualized risk scoring, placement of customers into risk categories or another means of assessing customer risk that allows firms to understand the risk posed by the customer and to demonstrate that understanding.

The CDD Rule also addresses the interplay of understanding the nature and purpose of customer relationships with the ongoing monitoring obligation discussed below. The CDD Rule explains that firms are not necessarily required or expected to integrate customer information or the customer risk profile into existing transaction monitoring systems (for example, to serve as the baseline for identifying and assessing suspicious transactions on a contemporaneous basis). Rather, FinCEN expects firms to use the customer information and customer risk profile as appropriate during the course of complying with their obligations under the BSA in order to determine whether a particular flagged transaction is suspicious.

TEXT EXAMPLE

We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile through the following methods [*describe*].

Depending on the facts and circumstances, a customer risk profile may include such information as:

- *The type of customer;*
- *The account or service being offered;*
- *The customer's income;*
- *The customer's net worth;*
- *The customer's domicile;*
- *The customer's principal occupation or business; and*
- *In the case of existing customers, the customer's history of activity.*

Rules: 31 C.F.R. § 1010.230; 31 C.F.R. § 1023.210(b)(5)(i).
Resources: FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (7/19/2016); Regulatory Notice 17-40.

c. Conducting Ongoing Monitoring to Identify and Report Suspicious Transactions

As with the requirement to understand the nature and purpose of the customer relationship, the requirement to conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including information regarding the beneficial ownership of legal entity

customers, merely adopts existing supervisory and regulatory expectations as explicit minimum standards of customer due diligence required for firms' AML programs. If, in the course of its normal monitoring for suspicious activity, the member firm detects information that is relevant to assessing the customer's risk profile, the member firm must update the customer information, including the information regarding the beneficial owners of legal entity customers, as discussed above. However, there is no expectation that the member firm update customer information, including beneficial ownership information, on an ongoing or continuous basis.

TEXT EXAMPLE

We will conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information, including information regarding the beneficial ownership of legal entity customers, using the customer risk profile as a baseline against which customer activity is assessed for suspicious transaction reporting. Our suspicious activity monitoring procedures are detailed within Section 11 (Monitoring Accounts for Suspicious Activity).

Rules: 31 C.F.R. § 1010.230; 31 C.F.R. § 1023.210(b)(5)(ii).
Resources: FIN-2016-G003: Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions (7/19/2016); Regulatory Notice 17-40.

7. Correspondent Accounts for Foreign Shell Banks

a. Detecting and Closing Correspondent Accounts of Foreign Shell Banks

Broker-dealers are prohibited from establishing, maintaining, administering or managing correspondent accounts in the United States for foreign shell banks. Broker-dealers also must take reasonable steps to ensure that any correspondent account established, maintained, administered or managed by the broker-dealer in the United States for a foreign bank is not being used by that foreign bank to indirectly provide banking services to a foreign shell bank. The BSA regulations allow covered financial institutions to receive a safe harbor for compliance with these requirements if they use the certification process described in the regulations. A covered financial institution must obtain a certification from each foreign bank for which it maintains a correspondent account "at least once every three years" to maintain the safe harbor.

In the context above, "correspondent account" is an account established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank.

Foreign shell banks are foreign banks without a physical presence in any country. A "foreign bank" is any bank organized under foreign law or an agency, branch or office of a bank located outside the U.S. The term does not include an agent, agency, branch or office within the U.S. of a bank organized under foreign law.

The prohibition does not include foreign shell banks that are regulated affiliates. Foreign shell banks that are regulated affiliates are affiliates of a depository institution, credit union or foreign bank that maintains a physical presence in the U.S., or a foreign country, and are subject to supervision by a banking authority in the country regulating that affiliated depository institution, credit union or foreign bank. Foreign branches of a U.S. broker-dealer are not subject to this requirement, and "correspondent accounts" of foreign banks that are clearly established, maintained, administered or managed only at foreign branches are not subject to this regulation.

Describe how your firm will identify foreign banks with which the firm has accounts, and then detect and close correspondent accounts for foreign shell banks.

NOTE: ***If your firm does not establish, maintain, administer or manage correspondent accounts for foreign banks, state that this is your firm's policy and describe the internal controls that your firm will implement to detect any attempt to open a correspondent account.***

TEXT EXAMPLE: We will identify foreign bank accounts and any such account that is a correspondent account (any account that is established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank) for foreign shell banks by [*describe procedure to detect such accounts*]. Upon finding or suspecting such accounts, firm employees will notify the AML Compliance Person, who will terminate any verified correspondent account in the United States for a foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by a foreign shell bank but is being used to provide services to such a shell bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period. We will terminate any correspondent account for which we have not obtained the information described in Appendix A of the regulations regarding shell banks within the time periods specified in those regulations.

Rule: 31 C.F.R. § 1010.630; 31 C.F.R. § 1010.605.

b. Certifications

Describe your process for obtaining certain required information from any foreign bank account holders and for obtaining the necessary certifications at least once every three years to rely on the safe harbor provided by the BSA regulations.

TEXT EXAMPLE: We will require our foreign bank account holders to identify the owners of the foreign bank if it is not publicly traded, the name and street address of a person who resides in the United States and is authorized and has agreed to act as agent for acceptance of legal process, and an assurance that the foreign bank is not a shell bank nor is it facilitating activity of a shell bank. In lieu of this information the foreign bank

may submit the Certification Regarding Correspondent Accounts For Foreign Banks provided in the BSA regulations. We will re-certify when we believe that the information is no longer accurate or at least once every three years.

Rule: 31 C.F.R. § 1010.630(b).
Resources: FinCEN's Chapter X web page; Certification Regarding Correspondent Accounts for Foreign Banks; Recertification Regarding Correspondent Accounts for Foreign Banks; FIN-2006-G003: Frequently Asked Questions: Foreign Bank Recertifications under 31 C.F.R. § 103.77 (2/3/2006).

c. Recordkeeping for Correspondent Accounts for Foreign Banks

Firms must keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

TEXT EXAMPLE: We will keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

Rule: 31 C.F.R. § 1010.630(e).

d. Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationships with Foreign Bank

The Secretary of the Treasury or the Attorney General of the United States may issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and may request records related to such correspondent account, including records maintained outside of the United States relating to the deposit of funds into the foreign bank. The summons or subpoena may be served on the foreign bank in the United States if the foreign bank has a representative in the United States, or in a foreign country pursuant to any mutual legal assistance treaty, multilateral agreement or other request for international law enforcement assistance.

A broker-dealer that maintains a correspondent account for a foreign bank in the United States must maintain records in the United States identifying the owners of such foreign bank whose shares are not publicly traded and the name and street address of a person who resides in the United States and is authorized, and has agreed to be an agent to accept service of legal process for the foreign bank's correspondent account. Upon receipt of a written request from a federal law enforcement officer for this information, the broker-dealer must provide such information to the requesting officer no later than seven days after receipt of the request.

Additionally, such broker-dealer must terminate any correspondent relationship with a foreign bank not later than 10 business days after receipt of written notice from the Secretary of the Treasury or the Attorney General of the United States that the foreign bank has failed to: (1) comply with a summons or subpoena issued by these two entities;

or (2) initiate proceedings in a United States court contesting such summons or subpoena.

Describe your firm's procedures for handling requests from federal law enforcement officers for the information described above, and if necessary, terminating a correspondent relationship with a foreign bank that has failed to comply or contest a summons or subpoena issued by the Secretary of the Treasury or the Attorney General of the United States.

TEXT EXAMPLE: When we receive a written request from a federal law enforcement officer for information identifying the non-publicly traded owners of any foreign bank for which we maintain a correspondent account in the United States and/or the name and address of a person residing in the United States who is an agent to accept service of legal process for a foreign bank's correspondent account, we will provide that information to the requesting officer not later than seven days after receipt of the request. We will close, within 10 days, any correspondent account for a foreign bank that we learn from FinCEN or the Department of Justice has failed to comply with a summons or subpoena issued by the Secretary of the Treasury or the Attorney General of the United States or has failed to contest such a summons or subpoena. We will scrutinize any correspondent account activity during that 10-day period to ensure that any suspicious activity is appropriately reported and to ensure that no new positions are established in these correspondent accounts.

Rule: *31 C.F.R. § 1010.670.*

8. Due Diligence and Enhanced Due Diligence Requirements for Correspondent Accounts of Foreign Financial Institutions

a. Due Diligence for Correspondent Accounts of Foreign Financial Institutions

The BSA, as amended by Section 312 of the USA PATRIOT Act, and the rules promulgated thereunder require, in part, that a firm, as part of its anti-money laundering program, establish a due diligence program that includes appropriate, specific, risk-based and, where necessary, enhanced policies, procedures and controls that are reasonably designed to enable the firm to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered or managed by the firm for a foreign financial institution.

A foreign financial institution is:

(1) a foreign bank;

(2) any branch or office located outside the United States of a broker-dealer; futures commission merchant or introducing broker; or open-end mutual fund company;

(3) any other person organized under foreign law (other than a branch or office of such person in the United States) that, if it were located in the United States,

would be a broker-dealer; futures commission merchant or introducing broker; or open-end mutual fund company; and

(4) any person organized under foreign law (other than a branch or office of such person in the United States) that is engaged in the business of, and is readily identifiable as: (a) a currency dealer or exchanger; or (b) a money transmitter.

A person, however, is not "engaged in the business" of a currency dealer, a currency exchanger or a money transmitter if such transactions are merely incidental to the person's business.

A "correspondent account" is defined in this context as any account established for a foreign financial institution to receive deposits from, or to make payments or other disbursement on behalf of, the foreign financial institution, or to handle other financial transactions for the foreign financial institution. "Account" is defined as any formal relationship established with a broker or dealer in securities to provide regular services to effect transactions in securities, including but not limited to, the purchase or sale of securities and securities loaned and borrowed activity, and to hold securities or other assets for safekeeping or as collateral.

For broker-dealers, correspondent accounts established on behalf of foreign financial institutions include, but are not limited to: (1) accounts to purchase, sell, lend, or otherwise hold securities, including securities repurchase programs; (2) prime brokerage accounts that clear and settle securities transactions for clients; (3) accounts for trading foreign currency; (4) custody accounts for holding securities or other assets in connection with securities transactions as collateral; and (5) over-the-counter derivative contracts.

On January 30, 2008, FinCEN issued guidance clarifying that covered financial institutions (which includes U.S. broker-dealers) presenting a negotiable instrument for payment to a foreign financial institution on which the instrument is drawn would not, by itself, be establishing a correspondent account between the covered financial institution and the paying institution. See FIN-2008-G001: Application of Correspondent Account Rules to the Presentation of Negotiable Instruments Received by a Covered Financial Institution for Payment (1/30/2008).

Describe your firm's due diligence program for any correspondent accounts established on behalf of foreign financial institutions.

TEXT EXAMPLE: We will conduct an inquiry to determine whether a foreign financial institution has a correspondent account established, maintained, administered or managed by the firm.

If we have correspondent accounts for foreign financial institutions, we will assess the money laundering risk posed, based on a consideration of relevant risk factors. We can apply all or a subset of these risk factors depending on the nature of the foreign financial institutions and the relative money laundering risk posed by such institutions.

The relevant risk factors can include:

- the nature of the foreign financial institution's business and the markets it serves;

- the type, purpose and anticipated activity of such correspondent account;

- the nature and duration of the firm's relationship with the foreign financial institution and its affiliates;

- the anti-money laundering and supervisory regime of the jurisdiction that issued the foreign financial institution's charter or license and, to the extent reasonably available, the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered; and

- information known or reasonably available to the covered financial institution about the foreign financial institution's anti-money laundering record.

In addition, our due diligence program will consider additional factors that have not been enumerated above when assessing foreign financial institutions that pose a higher risk of money laundering.

We will apply our risk-based due diligence procedures and controls to each financial foreign institution correspondent account on an ongoing basis. This includes periodically reviewing the activity of each foreign financial institution correspondent sufficient to ensure whether the nature and volume of account activity is generally consistent with the information regarding the purpose and expected account activity and to ensure that the firm can adequately identify suspicious transactions. Ordinarily, we will not conduct this periodic review by scrutinizing every transaction taking place within the account. One procedure we may use instead is to use any account profiles for our correspondent accounts (to the extent we maintain these) that we ordinarily use to anticipate how the account might be used and the expected volume of activity to help establish baselines for detecting unusual activity. [*Describe in detail all of the firm's procedures for periodically reviewing foreign financial institution account activity*].

OR:

We have reviewed our accounts and we do not have, nor do we intend to open or maintain, correspondent accounts for foreign financial institutions [*and describe the internal controls that your firm will implement to detect any attempt to open one of these types of accounts*].

Rule: 31 C.F.R. § 1010.610(a).

Resource: *FIN-2006-G009: Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries (5/10/2006)*.

b. Enhanced Due Diligence

The BSA, as amended by Section 312 of the USA PATRIOT Act, and the rules promulgated thereunder require, in part, that a firm's due diligence program for correspondent accounts of foreign financial institutions include the performance of enhanced due diligence on correspondent accounts for any foreign bank that operates under:

(1) an offshore banking license;
(2) a banking license issued by a foreign country that has been designated as non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization of which the United States is a member and with which designation the U.S. representative to the group or organization concurs; or
(3) a banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

TEXT EXAMPLE: We will assess any correspondent accounts for foreign financial institutions to determine whether they are correspondent accounts that have been established, maintained, administered or managed for any foreign bank that operates under:

(1) an offshore banking license;
(2) a banking license issued by a foreign country that has been designated as non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization of which the United States is a member and with which designation the U.S. representative to the group or organization concurs; or
(3) a banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

If we determine that we have any correspondent accounts for these specified foreign banks, we will perform enhanced due diligence on these correspondent accounts. The enhanced due diligence that we will perform for each correspondent account will include, at a minimum, procedures to take reasonable steps to:

(1) conduct enhanced scrutiny of the correspondent account to guard against money laundering and to identify and report any suspicious transactions. Such scrutiny will not only reflect the risk assessment that is described in Section 8.a. above, but will also include procedures to, as appropriate:

(i) obtain (*e.g.*, using a questionnaire) and consider information related to the foreign bank's AML program to assess the extent to which the foreign bank's correspondent account may expose us to any risk of money laundering;

(ii) monitor transactions to, from or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity (this monitoring may be conducted manually or electronically and may be done on an individual account basis or by product activity); and

(iii) obtain information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account (a correspondent account maintained for a foreign bank through which the foreign bank permits its customer to engage, either directly or through a subaccount, in banking activities) and the sources and beneficial owners of funds or other assets in the payable-through account.

(2) determine whether the foreign bank maintains correspondent accounts for other foreign banks that enable those other foreign banks to gain access to the correspondent account under review and, if so, to take reasonable steps to obtain information to assess and mitigate the money laundering risks associated with such accounts, including, as appropriate, the identity of those other foreign banks; and

(3) if the foreign bank's shares are not publicly traded, determine the identity of each owner and the nature and extent of each owner's ownership interest. We understand that for purposes of determining a private foreign bank's ownership, an "owner" is any person who directly or indirectly owns, controls or has the power to vote 10 percent or more of any class of securities of a foreign bank. We also understand that members of the same family shall be considered to be one person.

Rule: 31 C.F.R. § 1010.610(b); 31 C.F.R. § 1010.610(c).

c. Special Procedures When Due Diligence or Enhanced Due Diligence Cannot Be Performed

A firm must include procedures to follow in circumstances where the firm cannot perform appropriate due diligence for a correspondent account of a foreign financial institution or the enhanced due diligence that is required for correspondent accounts for certain foreign banks.

TEXT EXAMPLE: In the event there are circumstances in which we cannot perform appropriate due diligence with respect to a correspondent account, we will determine, at a minimum, whether to refuse to open the account, suspend transaction activity, file a SAR-SF, close the correspondent account and/or take other appropriate action.

Rule: 31 C.F.R. § 1010.610(d).

9. Due Diligence and Enhanced Due Diligence Requirements for Private Banking Accounts/Senior Foreign Political Figures

Describe your firm's due diligence program for "private banking" accounts for non-U.S. persons. Firms must have a due diligence program that is reasonably designed to detect and report any known or suspected money laundering conducted through or involving any private banking account maintained by or on behalf of a non-U.S. person, as well as the existence of the proceeds of foreign corruption in any such account. This requirement applies to all private banking accounts for non-U.S. persons, regardless of when they were opened. Accounts requested or maintained by or on behalf of "senior foreign political figures," which is defined below and includes their immediate family members and close known associates, require enhanced scrutiny. Senior foreign political figures are often referred to as "politically exposed persons" or "PEPs."

A "private banking" account is an account (or any combination of accounts) that requires a minimum aggregate deposit of $1,000,000, is established for one or more individuals and is assigned to or administered or managed by, in whole or in part, an officer, employee or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

A "senior foreign political figure" includes a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned commercial enterprise; a corporation, business, or other entity formed by or for the benefit of any such individual; an immediate family member of such an individual; or any individual widely and publicly known (or actually known by the firm) to be a close personal or professional associate of such an individual.

NOTE: ***If your firm does not open or maintain private banking accounts, state that this is your firm's policy.***

TEXT EXAMPLE:

EITHER:

We will review our accounts to determine whether we offer any private banking accounts and we will conduct due diligence on such accounts. This due diligence will include, at least: (1) ascertaining the identity of all nominal holders and holders of any beneficial

ownership interest in the account (including information on those holders' lines of business and sources of wealth); (2) ascertaining the source of funds deposited into the account; (3) ascertaining whether any such holder may be a senior foreign political figure; and (4) detecting and reporting, in accordance with applicable laws and regulations, any known or suspected money laundering, or use of the proceeds of foreign corruption.

We will review public information, including information available in Internet databases, to determine whether any private banking account holders are senior foreign political figures. If we discover information indicating that a particular private banking account holder may be a senior foreign political figure, and upon taking additional reasonable steps to confirm this information, we determine that the individual is, in fact, a senior foreign political figure, we will conduct additional enhanced due diligence to detect and report transactions that may involve money laundering or the proceeds of foreign corruption.

In so doing, we will consider the risks that the funds in the account may be the proceeds of foreign corruption by determining the purpose and use of the private banking account, location of the account holder(s), source of funds in the account, type of transactions conducted through the account and jurisdictions involved in such transactions. The degree of scrutiny we will apply will depend on various risk factors, including, but not limited to, whether the jurisdiction the senior foreign political figure is from is one in which current or former political figures have been implicated in corruption and the length of time that a former political figure was in office. Our enhanced due diligence might include, depending on the risk factors, probing the account holder's employment history, scrutinizing the account holder's source(s) of funds, and monitoring transactions to the extent necessary to detect and report proceeds of foreign corruption, and reviewing monies coming from government, government controlled or government enterprise accounts (beyond salary amounts).

If we do not find information indicating that a private banking account holder is a senior foreign political figure, and the account holder states that he or she is not a senior foreign political figure, then we may make an assessment if a higher risk for money laundering, nevertheless, exists independent of the classification. If a higher risk is apparent, we will consider additional due diligence measures such as [*describe in detail the additional measures*].

In either case, if due diligence (or the required enhanced due diligence, if the account holder is a senior foreign political figure) cannot be performed adequately, we will, after consultation with the firm's AML Compliance Person and, as appropriate, not open the account, suspend the transaction activity, file a SAR-SF, close the account and/or take other appropriate action.

OR:

We do not open or maintain private banking accounts.

Rule: 31 C.F.R. § 1010.620.
Resources: Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption (1/1/2001); FIN-2008-G005: Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Political Corruption (4/17/2008).

10. Compliance with FinCEN's Issuance of Special Measures Against Foreign Jurisdictions, Financial Institutions or International Transactions of Primary Money Laundering Concern

Describe how your firm will comply with the BSA, as amended by Section 311 of the USA PATRIOT Act, which grants the Secretary of the Treasury the authority, after finding that reasonable grounds exist for concluding that (1) a jurisdiction outside of the United States; (2) one or more financial institutions operating outside of the United States; (3) one or more classes of transactions within, or involving, a jurisdiction outside of the United States; or (4) one or more types of accounts is of "primary money laundering concern," to require domestic financial institutions, such as broker-dealers, to take certain "special measures" against the primary money laundering concern. There is a special section on the FinCEN website where all the Section 311 designations are listed. See Section 311 – Special Measures.

TEXT EXAMPLE:

EITHER:

We do not maintain any accounts (including correspondent accounts) with any foreign jurisdiction or financial institution. However, if FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes of international transactions or types of accounts deeming them to be of primary money laundering concern, we understand that we must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule.

OR:

If FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes of international transactions or types of accounts deeming them to be of primary money laundering concern, we understand that we must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule. For example, if the final rule deems a certain bank and its subsidiaries (Specified Banks) to be of primary money laundering concern, a special measure may be a prohibition from opening or maintaining a correspondent account in the United States for, or on behalf of, the Specified Banks. In that case, we will take the following steps:

(1) We will review our account records, including correspondent account records, to ensure that our accountholders and correspondent accountholders maintain no accounts directly for, or on behalf of, the Specified Banks; and

(2) We will apply due diligence procedures to our correspondent accounts that are reasonably designed to guard against indirect use of those accounts by the Specified Banks. Such due diligence may include:

- Notification to Correspondent Accountholders

  We will notify our correspondent accountholders that the account may not be used to provide the Specified Banks with access to us [*provide details of what the language of the notice will state*].

  We will transmit the notice to our correspondent accounts using the following method [*specify*], and we shall retain documentation of such notice.

- Identification of Indirect Use

  We will take reasonable steps in order to identify any indirect use of our correspondent accounts by the Specified Banks. We will determine if such indirect use is occurring from transactional records that we maintain in the normal course of business. We will take a risk-based approach when deciding what, if any, additional due diligence measures we should adopt to guard against the indirect use of correspondent accounts by the Specified Banks, based on risk factors such as the type of services offered by, and geographic locations of, their correspondents.

  We understand that we have an ongoing obligation to take reasonable steps to identify all correspondent account services our correspondent accountholders may directly or indirectly provide to the Specified Banks.

Rules: 31 C.F.R. §§ 1010.651, 1010.653, 1010.655, 1010.658, 1010.659, 1010.660.Resources: Section 311 – Special Measures (for information on all special measures issued by FinCEN); NTM 07-17; NTM 06-41.

11. Monitoring Accounts for Suspicious Activity

Broker-dealers must establish risk-based procedures reasonably designed to detect and report suspicious transactions in order to comply with the BSA and FINRA Rule 3310.

These procedures must include using the customer's risk profile as a baseline to monitor for suspicious activity. The risk of suspicious activity will vary for each firm depending on its size and location and based on its business model and the products and services it offers. Your firm can identify that risk by looking at the type of customers it serves, where its customers are located, and the types of products and services it offers. Given the wide variety of business models employed by small firms, it is paramount that your firm's monitoring procedures be tailored to your firm's business and identified risks. Additionally, your procedures should identify "red flags" or indicators of possible suspicious activity to identify circumstances warranting further due diligence by the firm. Higher risk accounts and transactions generally need to be subjected to greater scrutiny.

Your procedures should also describe how the firm will monitor for or otherwise identify these "red flags." Your firm may monitor transactions manually or through automated systems or a combination of the two, as long as the system is reasonably designed to identify and report suspicious activity. Note that the types of suspicious activity that are reportable on SAR-SF are very broad and include, among other things, securities fraud.

It is important that your procedures provide specific details regarding your firm's monitoring system (e.g., who, what, when, where and how).

TEXT EXAMPLE:

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. (Red flags are identified in Section 11.b. below.) Monitoring will be conducted through the following methods: [*describe*]. [*If automated monitoring is utilized, your procedures should include a list of reports as well as their purpose and description. If manual monitoring is utilized, your procedures should include a list of documents/systems to be reviewed and the purpose of the review. Regardless of the method, your procedures should address how this monitoring will be conducted and the frequency with which it will be conducted.*] The customer risk profile will serve as a baseline for assessing potentially suspicious activity. The AML Compliance Person or his or her designee [*Add if appropriate: in consultation with {Name or title} OR with the approval of {Name or title}*] will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

We will conduct the following reviews of activity that our monitoring system detects: [*describe*]. We will document our monitoring and reviews as follows: [*describe*]. The AML Compliance Person or his or her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR-SF is filed. Relevant information can include, but not be limited to, the following: [*describe*].

Rules: 31 C.F.R. § 1023.320; FINRA Rule 3310.

Resource: 67 Fed. Reg. 44048 (July 1, 2002) (Final Rule: Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations – Requirement that Brokers or Dealers in Securities Report Suspicious Transactions) it is intended that broker-dealers, and indeed every type of financial institution to which the suspicious transaction reporting rules of 31 CFR part 103 apply, will evaluate customer activity and relationships for money laundering risks, and design a suspicious transaction monitoring program that is appropriate for the particular broker-dealer in light of such risks").

a. Emergency Notification to Law Enforcement by Telephone

Describe when and how your firm will call the appropriate law enforcement authority in emergencies.

TEXT EXAMPLE: In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority. If a customer or company appears on OFAC's SDN list, we will call the OFAC Hotline at (800) 540-6322. Other contact numbers we will use are: FinCEN's Financial Institutions Hotline ((866) 556-3974) (especially to report transactions relating to terrorist activity), local U.S. Attorney's office (*insert contact number),* local FBI office (*insert contact number)* and local SEC office (*insert contact number)* (to voluntarily report such violations to the SEC in addition to contacting the appropriate law enforcement authority). If we notify the appropriate law enforcement authority of any such activity, we must still file a timely SAR-SF.

Although we are not required to, in cases where we have filed a SAR-SF that may require immediate attention by the SEC, we may contact the SEC via the SEC SAR Alert Message Line at (202) 551-SARS (7277) to alert the SEC about the filing. We understand that calling the SEC SAR Alert Message Line does not alleviate our obligations to file a SAR-SF or notify an appropriate law enforcement authority.

Rule: 31 C.F.R. § 1023.320.
Resources: *FinCEN's website*; *OFAC web page*; *NTM 02-21; NTM 02-47.*

b. Red Flags

TEXT EXAMPLE: Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

Customers – Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.

- Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.

- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.

- Background is questionable or differs from expectations based on business activities.

- Customer with no discernable reason for using the firm's service.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.

- Tries to persuade an employee not to file required reports or not to maintain required records.

- "Structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.

- Unusual concern with the firm's compliance with government reporting requirements and firm's AML policies.

Certain Funds Transfer Activities

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.

- Many small, incoming wire transfers or deposits made using checks and money orders. Almost immediately withdrawn or wired out in manner inconsistent with customer's business or history. May indicate a Ponzi scheme.

- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

Certain Deposits or Dispositions of Physical Certificates

- Physical certificate is titled differently than the account.

- Physical certificate does not bear a restrictive legend, but based on history of the stock and/or volume of shares trading, it should have such a legend.

- Customer's explanation of how he or she acquired the certificate does not make sense or changes.

- Customer deposits the certificate with a request to journal the shares to multiple accounts, or to sell or otherwise transfer ownership of the shares.

Certain Securities Transactions

- Customer engages in prearranged or other non-competitive trading, including wash or cross trades of illiquid securities.
- Two or more accounts trade an illiquid stock suddenly and simultaneously.
- Customer journals securities between unrelated accounts for no apparent business reason.
- Customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.
- Customer transactions include a pattern of receiving stock in physical form or the incoming transfer of shares, selling the position and wiring out proceeds.
- Customer's trading patterns suggest that he or she may have inside information.

Transactions Involving Penny Stock Companies

- Company has no business, no revenues and no product.
- Company has experienced frequent or continuous changes in its business structure.
- Officers or insiders of the issuer are associated with multiple penny stock issuers.
- Company undergoes frequent material changes in business strategy or its line of business.
- Officers or insiders of the issuer have a history of securities violations.
- Company has not made disclosures in SEC or other regulatory filings.
- Company has been the subject of a prior trading suspension.

Transactions Involving Insurance Products

- Cancels an insurance contract and directs funds to a third party.
- Structures withdrawals of funds following deposits of insurance annuity checks signaling an effort to avoid BSA reporting requirements.
- Rapidly withdraws funds shortly after a deposit of a large insurance check when the purpose of the fund withdrawal cannot be determined.

- Cancels annuity products within the free look period which, although could be legitimate, may signal a method of laundering funds if accompanied with other suspicious indicia.

- 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.

- Purchases an insurance product with no concern for investment objective or performance.

- Purchases an insurance product with unknown or unverifiable sources of funds, such as cash, official checks or sequentially numbered money orders.

Activity Inconsistent With Business

- Transactions patterns show a sudden change inconsistent with normal activities.

- Unusual transfers of funds or journal entries among accounts without any apparent business purpose.

- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.

- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

Other Suspicious Customer Activity

- Unexplained high level of account activity with very low levels of securities transactions.

- Funds deposits for purchase of a long-term investment followed shortly by a request to liquidate the position and transfer the proceeds out of the account.

- Law enforcement subpoenas.

- Large numbers of securities transactions across a number of jurisdictions.

- Buying and selling securities with no purpose or in unusual circumstances (*e.g.*, churning at customer's request).

- Payment by third-party check or money transfer without an apparent connection to the customer.

- Payments to third-party without apparent connection to customer.

- No concern regarding the cost of transactions or fees (*i.e.*, surrender fees, higher than necessary commissions, etc.).

c. Responding to Red Flags and Suspicious Activity

TEXT EXAMPLE: When an employee of the firm detects any red flag, or other activity that may be suspicious, he or she will notify [*include procedures for escalation of suspicious activity*]. Under the direction of the AML Compliance Person, the firm will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a SAR-SF.

12. Suspicious Transactions and BSA Reporting

Describe your firm's procedures for identifying any suspicious transactions and determining if they need further investigation or warrant filing a SAR-SF. These procedures should also cover the maintenance of SAR documentation and the preservation of its confidentiality, and BSA reporting. Note that firms must exercise due diligence in monitoring suspicious activity as the regulations require firms to file a SAR-SF when they "know, suspect, or have reason to suspect" that transactions involve certain suspicious activities.

Firms are exempt from reporting on a SAR-SF the following violations: (1) a robbery or burglary that is committed or attempted and already reported to appropriate law enforcement authorities; (2) lost, missing, counterfeit or stolen securities that the firm has reported pursuant to Exchange Act Rule 17f-1; and (3) violations of the Federal securities laws or self-regulatory organization (SRO) rules by the firm, its officers, directors, employees or registered representatives, that are reported appropriately to the SEC or SRO, except for a violation of Exchange Act Rule 17a-8, which must be reported on a SAR-SF. However, if a firm relies on one of these exemptions, it may be required to demonstrate that it relied on one of these exemptions and must maintain records, for at least five years, of its determination not to file a SAR-SF based on the exemption.

Rule: 31 C.F.R. § 1023.320.

a. Filing a SAR-SF

TEXT EXAMPLE: We will file SAR-SFs with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at or through our firm involving $5,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect or have reason to suspect:

(1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity

as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
(2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the BSA regulations;
(3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or
(4) the transaction involves the use of the firm to facilitate criminal activity.

We will also file a SAR-SF and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. In addition, although we are not required to, we may contact that SEC in cases where a SAR-SF we have filed may require immediate attention by the SEC. *See* Section 11 for contact numbers. We also understand that, even if we notify a regulator of a violation, unless it is specifically covered by one of the exceptions in the SAR rule, we must file a SAR-SF reporting the violation.

We may file a voluntary SAR-SF for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the SAR rule. It is our policy that all SAR-SFs will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the SAR-SF.

We will report suspicious transactions by completing a SAR-SF, and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR-SF. If no suspect is identified on the date of initial detection, we may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. The phrase "initial detection" does not mean the moment a transaction is highlighted for review. The 30-day (or 60-day) period begins when an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

We will retain copies of any SAR-SF filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, federal or state securities regulators or SROs upon request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR-SF or the information contained in the SAR-

SF will, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency, or an SRO registered with the SEC, decline to produce the SAR-SF or to provide any information that would disclose that a SAR-SF was prepared or filed. We will notify FinCEN of any such request and our response.

Rules: 31 C.F.R. § 1023.320; FINRA Rule 3310.
Resources: FinCEN's website contains additional information, including information on the BSA E-Filing System, the FinCEN Suspicious Activity Report: Introduction and Filing Instructions, and the biannual SAR Activity Review – Trends, Tips & Issues, which discusses trends in suspicious reporting and gives helpful tips; The SAR Activity Review, Issue 10 (May 5/2006) (documentation of decision not to file a SAR; grand jury subpoenas and suspicious activity reporting, and commencement of 30-day time period to file a SAR); FinCEN SAR Narrative Guidance Package (11/2003), FinCEN Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting (10/10/2007); NTM 02-21; NTM 02-47.

b. Currency Transaction Reports

A firm must file a currency transaction report (CTR) for each deposit, withdrawal, exchange of currency, or other payment or transfer by, through or to the firm that involves a transaction in currency of more than $10,000 or for multiple transactions in currency of more than $10,000 when a financial institution knows that the transactions are by or on behalf of the same person during any one business day, unless the transaction is subject to certain exemptions. "Currency" is defined as "coin and currency of the United States or of any other country" that is "customarily used and accepted as money in the country in which issued; and a cashier's check (by whatever name called, including 'treasurer's check' and 'bank check'), bank draft, traveler's check, or money order having a face amount of not more than $10,000 received in a designated reporting transaction . . . or received in any transaction in which the recipient knows that such instrument is being used in an attempt to avoid the reporting of the transaction."

TEXT EXAMPLE: [*Include this language if your firm prohibits transactions involving currency]* Our firm prohibits transactions involving currency and has the following procedures to prevent such transactions: [*Describe*]. If we discover such transactions have occurred, we will file with FinCEN CTRs for currency transactions that exceed $10,000. Also, we will treat multiple transactions involving currency as a single transaction for purposes of determining whether to file a CTR if they total more than $10,000 and are made by or on behalf of the same person during any one business day. We will use the *BSA E-Filing System* to file the supported CTR Form.

Rules: 31 C.F.R. §§ 1010.311, 1010.306, 1010.312.
Resource: BSA E-Filing System; BSA E-Filing System Filing Instructions (including instructions for FinCEN CTR Form 112).

c. Currency and Monetary Instrument Transportation Reports

A currency and monetary instrument transportation report (CMIR) must be filed whenever more than $10,000 in currency or other monetary instruments is physically transported, mailed or shipped into or from the United States. A CMIR also must be filed whenever a person receives more than $10,000 in currency or other monetary instruments that has been physically transported, mailed or shipped from outside the United States and a CMIR has not already been filed with respect to the currency or other monetary instruments received. A CMIR is not required to be filed by a securities broker-dealer mailing or shipping currency or other monetary instruments through the postal service or by common carrier. "Monetary instruments" include the following: currency (defined above); traveler's checks in any form; all negotiable instruments (including personal and business checks, official bank checks, cashier's checks, third-party checks, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee or otherwise in such form that title passes upon delivery; incomplete negotiable instruments that are signed but omit the payee's name; and securities or stock in bearer form or otherwise in such form that title passes upon delivery.

TEXT EXAMPLE: [*Include this language if your firm prohibits both the receipt of currency or other monetary instruments that have been transported, mailed or shipped to the firm from outside of the United States and the physical transportation, mailing or shipment of currency or other monetary instruments by any means other than through the postal service or by common carrier*:] Our firm prohibits both the receipt of currency or other monetary instruments that have been transported, mailed or shipped to us from outside of the United States, and the physical transportation, mailing or shipment of currency or other monetary instruments by any means other than through the postal service or by common carrier. We will file a CMIR with the Commissioner of Customs if we discover that we have received or caused or attempted to receive from outside of the U.S. currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time (on one calendar day or, if for the purposes of evading reporting requirements, on one or more days). We will also file a CMIR if we discover that we have physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means other than through the postal service or by common carrier currency or other monetary instruments of more than $10,000 at one time (on one calendar day or, if for the purpose of evading the reporting requirements, on one or more days). We will use the CMIR Form provided on FinCEN's website.

Rules: 31 C.F.R. §§ 1010.340, 1010.306.
Resource: BSA E-Filing System.

d. Foreign Bank and Financial Accounts Reports

The regulations under the BSA require broker-dealers to report and keep records related to any financial interest in, or signature authority over, a bank account, securities account or other financial account that the firm has in a foreign country in which the aggregate value of any accounts exceed $10,000.

TEXT EXAMPLE: We will file a Foreign Bank and Financial Accounts Report (FBAR) for any financial accounts of more than $10,000 that we hold, or for which we have signature or other authority over, in a foreign country. We will use the BSA E-Filing System provided on FinCEN's website.

Rules: 31 C.F.R. §§ 1010.306, 1010.350, 1010.420.
Resource: BSA E-Filing System.

e. Monetary Instrument Purchases

No financial institution may issue or sell a bank check or draft, cashier's check, money order or traveler's check for $3,000 to $10,000 inclusive in currency unless it obtains and records certain information when issuing or selling one or more of these instruments to any individual purchaser. A financial institution issuing or selling one or more of these instruments to any individual purchaser in excess of $10,000 will also need to file a CTR. See Section 12.b.

TEXT EXAMPLE:

EITHER:

We do not issue bank checks or drafts, cashier's checks, money orders or traveler's checks in the amount of $3,000 or more.

OR:

When we issue or sell a bank check or draft, cashier's check, money order or traveler's check in the amounts of $3,000 to $10,000 inclusive, we will maintain records of the following information:

(a) (1) If the purchaser has a deposit account with us:

(i) (A) the name of the purchaser;

(B) the date of purchase;

(C) the type(s) of instrument(s) purchased;

(D) the serial number(s) of each of the instrument(s) purchased; and

(E) the amount in dollars of each of the instrument(s) purchased.

(ii) In addition, we must verify that the individual is a deposit accountholder or must verify the individual's identity. Verification

may be either through a signature card or other file or record provided the deposit accountholder's name and address were verified previously and that information was recorded on the signature card or other file or record; or by examination of a document which is normally acceptable as a means of identification when cashing checks for nondepositors and which contains the name and address of the purchaser. If the deposit accountholder's identity has not been verified previously, we shall verify the deposit accountholder's identity by examination of a document which is normally acceptable within the community as a means of identification when cashing checks for nondepositors and which contains the name and address of the purchaser, and shall record the specific identifying information (*e.g.*, driver's license number and state of issuance).

(2) If the purchaser does not have a deposit account with us:

(i) (A) the name and address of the purchaser;

(B) the Social Security number of the purchaser, or if the purchaser is an alien and does not have a Social Security number, the alien identification number;

(C) the date of birth of the purchaser;

(D) the date of purchase;

(E) the type(s) of instrument(s) purchased;

(F) the serial number(s) of the instrument(s) purchased; and

(G) the amount in dollars of each of the instrument(s) purchased.

(ii) In addition, we shall verify the purchaser's name and address by examination of a document which is normally acceptable within the community as a means of identification when cashing checks for nondepositors and which contains the name and address of the purchaser, and shall record the specific identifying information (*e.g.*, driver's license number and state of issuance).

(b) Contemporaneous purchases of the same or different types of instruments totaling $3,000 or more shall be treated as one purchase. Multiple purchases during one business day totaling $3,000 or more shall be treated as one purchase if an individual employee, director, officer or partner of the [*Name of Firm*] has knowledge that these purchases have occurred.

(c) We shall keep records required to be kept for a period of five years, and such records shall be made available to the federal and state authorities or SROs upon request at any time.

Rule: 31 C.F.R. § 1010.415.
Resource: 59 Fed. Reg. 52250 (October 17, 1994) (Final Rule; Amendments to BSA Regulations Relating to Identification Required to Purchase Bank Checks and Drafts, Cashier's Checks, Money Orders, and Traveler's Checks).

f. Funds Transmittals of $3,000 or More Under the Travel Rule

TEXT EXAMPLE: When we are the transmittor's financial institution in funds of $3,000 or more, we will retain either the original or a copy (*e.g.*, microfilm, electronic record) of the transmittal order. We will also record on the transmittal order the following information: (1) the name and address of the transmittor; (2) if the payment is ordered from an account, the account number; (3) the amount of the transmittal order; (4) the execution date of the transmittal order; and (5) the identity of the recipient's financial institution. In addition, we will include on the transmittal order as many of the following items of information as are received with the transmittal order: (1) the name and address of the recipient; (2) the account number of the recipient; (3) any other specific identifier of the recipient; and (4) any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

We will also verify the identity of the person placing the transmittal order (if we are the transmitting firm), provided the transmittal order is placed in person and the transmittor is not an established customer of the firm (*i.e.*, a customer of the firm who has not previously maintained an account with us or for whom we have not obtained and maintained a file with the customer's name, address, taxpayer identification number, or, if none, alien identification number or passport number and country of issuance). If a transmittor or recipient is conducting business in person, we will obtain: (1) the person's name and address; (2) the type of identification reviewed and the number of the identification document (*e.g.*, driver's license); and (3) the person's taxpayer identification number (*e.g.*, Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record the lack thereof. If a transmittor or recipient is not conducting business in person, we shall obtain the person's name, address, and a copy or record of the method of payment (*e.g.*, check or credit card transaction). In the case of transmittors only, we shall also obtain the transmittor's taxpayer identification number (*e.g.*, Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. In the case of recipients only, we shall obtain the name and address of the person to which the transmittal was sent.

Rules: 31 C.F.R. § 1010.410(e) and (f); Exchange Act Rule 17a-8 (requiring registered broker-dealers subject to the Currency and Foreign Transactions Reporting Act of 1970

to comply with the BSA regulations regarding reporting, recordkeeping and record retention requirements); FINRA Rule 3310.

13. AML Recordkeeping

a. Responsibility for Required AML Records and SAR-SF Filing

Your firm must establish procedures to maintain all applicable AML program records and reviews.

TEXT EXAMPLE: Our AML Compliance Person and his or her designee will be responsible for ensuring that AML records are maintained properly and that SAR-SFs are filed as required.

In addition, as part of our AML program, our firm will create and maintain SAR-SFs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification *(See* Section 5 above) and funds transmittals. We will maintain SAR-SFs and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other recordkeeping requirements, including certain SEC rules that require six-year retention periods (*e.g.*, Exchange Act Rule 17a-4(a) requiring firms to preserve for a period of not less than six years, all records required to be retained by Exchange Act Rule 17a-3(a)(1)-(3), (a)(5), and (a)(21)-(22) and Exchange Act Rule 17a-4(e)(5) requiring firms to retain for six years account record information required pursuant to Exchange Act Rule 17a-3(a)(17)).

Rules: 31 C.F.R. § 1010.430; Exchange Act Rule 17a-8 (requiring registered broker-dealers subject to the Currency and Foreign Transactions Reporting Act of 1970 to comply with the BSA regulations regarding reporting, recordkeeping and record retention requirements); FINRA Rule 3310.

b. SAR-SF Maintenance and Confidentiality

Describe your firm's retention and confidentiality requirements for SAR-SFs.

TEXT EXAMPLE: We will hold SAR-SFs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, the SEC, an SRO registered with the SEC or other appropriate law enforcement or regulatory agency about a SAR-SF. We will refuse any subpoena requests for SAR-SFs or for information that would disclose that a SAR-SF has been prepared or filed and immediately notify FinCEN of any such subpoena requests that we receive. *See* Section 11 for contact numbers. We will segregate SAR-SF filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR-SF filings. Our AML Compliance Person will handle all subpoenas or other requests for SAR-SFs. [*Describe any other retention or confidentiality procedures of your firm for SAR-SFs.*] We may share information with another financial institution about suspicious transactions in order to determine whether we will jointly file a SAR according to the provisions of Section 3.d. In cases in which

we file a joint SAR for a transaction that has been handled both by us and another financial institution, both financial institutions will maintain a copy of the filed SAR.

Rule: 31 C.F.R. § 1023.320(e).
Resources: 67 Fed. Reg. 44048 (July 1, 2002) (Final Rule; Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations – Requirement that Brokers or Dealers in Securities Report Suspicious Transactions); NTM 02-47.

c. Additional Records

A firm is required to retain either an original or a microfilm or other copy or reproduction of certain records.

TEXT: We shall retain either the original or a microfilm or other copy or reproduction of each of the following:

- A record of each extension of credit in an amount in excess of $10,000, except an extension of credit secured by an interest in real property. The record shall contain the name and address of the person to whom the extension of credit is made, the amount thereof, the nature or purpose thereof and the date thereof;

- A record of each advice, request or instruction received or given regarding any transaction resulting (or intended to result and later canceled if such a record is normally made) in the transfer of currency or other monetary instruments, funds, checks, investment securities or credit, of more than $10,000 to or from any person, account or place outside the U.S.;

- A record of each advice, request or instruction given to another financial institution (which includes broker-dealers) or other person located within or without the U.S., regarding a transaction intended to result in the transfer of funds, or of currency, other monetary instruments, checks, investment securities or credit, of more than $10,000 to a person, account or place outside the U.S.;

- Each document granting signature or trading authority over each customer's account;

- Each record described in Exchange Act Rule 17a-3(a): (1) (blotters), (2) (ledgers for assets and liabilities, income, and expense and capital accounts), (3) (ledgers for cash and margin accounts), (4) (securities log), (5) (ledgers for securities in transfer, dividends and interest received, and securities borrowed and loaned), (6) (order tickets), (7) (purchase and sale tickets), (8) (confirms), and (9) (identity of owners of cash and margin accounts);

- A record of each remittance or transfer of funds, or of currency, checks, other monetary instruments, investment securities or credit, of more than $10,000 to a person, account or place, outside the U.S.; and

- A record of each receipt of currency, other monetary instruments, checks or investment securities and of each transfer of funds or credit, of more than $10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside the U.S.

Rules: 31 C.F.R. § 1010.410; 31 C.F.R. 1023.410; Exchange Act Rule 17a-8 (requiring registered broker-dealers subject to the Currency and Foreign Transactions Reporting Act of 1970 to comply with the BSA regulations regarding reporting, recordkeeping and record retention requirements); FINRA Rule 3310.

14. Clearing/Introducing Firm Relationships

Describe how you and your clearing firm will comply with your independent AML obligations, which include describing the exception reports, if any, you obtain from your clearing firm, how frequently the reports will be reviewed and by whom, what review or inquiry will be conducted regarding exceptions, and how that review will be evidenced.

TEXT EXAMPLE: We will work closely with our clearing firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply [with our contractual obligations and] with AML laws. Both our firm and our clearing firm have filed (and kept updated) the necessary annual certifications for such information sharing, which can be found on FinCEN's website. As a general matter, we will obtain and use the following exception reports offered by our clearing firm in order to monitor customer activity [*identify reports and the manner in which they will be used*] and we will provide our clearing firm with proper customer identification and due diligence information as required to successfully monitor customer transactions. We have discussed how each firm will apportion customer and transaction functions and how we will share information and set forth our understanding in a written document. We understand that the apportionment of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the BSA and its implementing regulations.

Rules: 31 CFR § 1010.540; FINRA Rule 3310; FINRA Rule 4311.
Resource: NTM 02-21.

15. Training Programs

Describe your AML ongoing employee training and programs.

TEXT EXAMPLE: We will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SAR-SFs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. Currently our training program is: [*insert specifics, such as "all registered representatives must view the video entitled "Spotting Money Laundering" by X date or within two weeks of being hired, etc.*] We will maintain records to show the persons trained, the dates of training and the subject matter of their training.

We will review our operations to see if certain employees, such as those in compliance, margin and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

Rules: 31 CFR § 1023.210(b)(4); FINRA Rule 3310.
Resources: See NTM 02-21, FinCEN SAR Narrative Guidance Package (11/01/2003); FinCEN Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting (10/10/2007).

16. Program to Independently Test AML Program

Describe your firm's independent testing function to assess its AML compliance program. You must choose whether your firm's personnel or a qualified outside party will perform this function. Your decision will depend on your firm's size and resources. Independent testing is generally to be performed annually (on a calendar year basis). A firm that does not execute transactions for customers or otherwise hold customer accounts and does not act as an introducing broker with respect to customer accounts (e.g., engages solely in proprietary trading or conducts business only with other broker-dealers) may generally perform an independent test every two calendar years. All firms should undertake more frequent testing than required if circumstances warrant.

As a general matter, independent testing of your firm's AML compliance program should include, at a minimum: (1) evaluating the overall integrity and effectiveness of your firm's AML compliance program; (2) evaluating your firm's procedures for BSA reporting and recordkeeping requirements; (3) evaluating the implementation and maintenance of your firm's CIP; (4) evaluating your firm's customer due diligence requirements; (5) evaluating your firm's transactions, with an emphasis on high-risk areas; (6) evaluating the adequacy of your firm's staff training program; (7) evaluating your firm's systems, whether automated or manual, for identifying suspicious activity; (8) evaluating your firm's system for reporting suspicious activity; (9) evaluating your firm's

policy for reviewing accounts that generate multiple SAR-SF filings; and (10) evaluating your firm's response to previously identified deficiencies.

a. Staffing

TEXT EXAMPLE*:*

EITHER

The testing of our AML program will be performed at least annually (on a calendar year basis) [*or if a firm is eligible, the firm may state "every two calendar years"*] by [*Name*], an independent third party. We will evaluate the qualifications of the independent third party to ensure they have a working knowledge of applicable requirements under the BSA and its implementing regulations. [*Name*] also has [*describe background in more detail*]. Independent testing will be performed more frequently if circumstances warrant.

OR

The testing of our AML program will be performed at least annually (on a calendar year basis) [*or, if the firm is eligible, every two calendar years*] by [*Names*], personnel of our firm, none of whom are [*who is not*] the AML Compliance Person nor do they [*he/she*] perform the AML functions being tested nor do they report to any such persons. Their [*his/her*] qualifications include a working knowledge of applicable requirements under the BSA and its implementing regulations [*and—describe any additional qualifications*]. To ensure that they [*he/she*] remain independent, we will separate their [*his/her*] functions from other AML activities by [*describe*]. Independent testing will be performed more frequently if circumstances warrant.

Rules: 31 C.F.R. § 1023.210(b)(2); FINRA Rule 3310.
Resource: NTM 06-07.

b. Evaluation and Reporting

TEXT EXAMPLE: After we have completed the independent testing, staff will report its findings to senior management [*or to an internal audit committee*]. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

Rules: 31 C.F.R. § 1023.210(b)(2); FINRA Rule 3310.

17. Monitoring Employee Conduct and Accounts

Describe how your firm will monitor employee accounts for potential signs of money laundering. Your firm must subject employee accounts to the same account identifying and monitoring procedures as customer accounts. Your firm should also review supervisors' performance of their AML responsibilities.

TEXT EXAMPLE: We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Person. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Person's accounts will be reviewed by [*Name – another member of senior management*.]

Rules: 31 C.F.R. § 1023.320; 31 C.F.R § 1023.210; FINRA Rule 3310.

18. Confidential Reporting of AML Non-Compliance

Describe how you ensure that employees who report suspected violations of AML compliance are protected from retaliation.

TEXT EXAMPLE: Employees will promptly report any potential violations of the firm's AML compliance program to the AML Compliance Person, unless the violations implicate the AML Compliance Person, in which case the employee shall report to [*the president/chairman of the board/audit committee chair*]. Such reports will be confidential, and the employee will suffer no retaliation for making them.

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310.

19. Additional Risk Areas

TEXT EXAMPLE: The firm has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above. The major additional areas of risk include [*describe*]. Additional procedures to address these major risks are [*describe*].

20. Senior Manager Approval

A firm's AML compliance program must be approved, in writing, by a member of senior management.

TEXT EXAMPLE: Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it. This approval is indicated by signatures below.

Rules: *31 C.F.R. § 1023.210; FINRA Rule 3310.*

Signed:

Title:

Date: