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.