Left of Boom: Fraud Prevention Solutions
Monday, May 16, 2022
11:15 a.m. – 12:15 p.m.

Join FINRA staff and industry experts as they discuss "left of boom". This means identifying the threat and preventing a disruption before an attack should occur. Panelists share effective left and right of boom policies and procedures.

Moderator:

Jamie Udinson
Senior Director, Strategic Alliances
FINRA Member Supervision

Panelists:

Jason Foye
Senior Director, Special Investigations Unit
FINRA Member Supervision

Ivy Gong
Global Head of Fraud Operations
Morgan Stanley

Kara Suro
Managing Director, Head of Fraud Risk Management
Charles Schwab & Co., Inc.

Tina Tambiah
Senior Director, Initial Review Group
FINRA Member Supervision

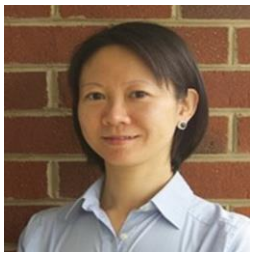
Left of Boom: Fraud Prevention Solutions Panelists Bios:

Moderator:

Jamie Udinson is Senior Director, Strategic Alliances in the Office of Member Supervision at FINRA, where she provides expert advice to the executive management team of Member Supervision, including the Executive Vice President of Member Supervision, on a full range of operational, policy and regulatory issues, and their associated communications. Ms. Udinson is responsible for strategic initiatives across Member Supervision's many groups, including Firm Exams, Risk Monitoring, the Member Application Program, and National Cause and Financial Crimes Detection Programs. During her 14 years at FINRA, Ms. Udinson has served in both the Member Supervision and Enforcement Departments, and most recently as the Chief of Staff to the Executive Vice President of National Cause and Financial Crimes Detection Program. Ms. Udinson has an MBA from La Salle University and is a Certified Anti-Money Laundering Specialist.

Panelists:

Jason Foye is Director of FINRA's AML Investigative Unit, a specialized team that conducts complex Anti-Money Laundering examinations, provides guidance to FINRA's examination and Enforcement staff in connection with AML-related matters, and provides education and training to FINRA staff and industry personnel throughout the country. Mr. Foye serves as an AML Regulatory Specialist within FINRA and is Certified Anti-Money Laundering Specialist and a Certified Fraud Examiner. Mr. Foye graduated from Florida State University with a Bachelor's degrees in Finance and Risk Management. Mr. Foye works from FINRA's Florida District Office, and has been with FINRA for 11 years.



Ivy Gong is the Global Head of Fraud Operations under Technology and Operations Risk Division at Morgan Stanley. In her current role, Ms. Gong is responsible for first-line fraud risk management for the firm, including fraud policy, strategy, analytics, investigation, and cyber fraud security awareness education. She also facilitates closer alignment of fraud and cyber synergy. Ms. Gong is based in Morgan Stanley Baltimore office. She joined the Global Fraud Operations in 2016 at the initial stage of the Fraud Operations function built out. Prior to Morgan Stanley, Ms. Gong has 15 plus years' experience in various risk management roles with retail banking, credit card, and management consulting.

Kara Suro is Managing Director and Head of Fraud Risk Management responsible for governance and implementation of Schwab's Fraud Risk Management Program, including orchestration of firm-wide fraud strategy prevention, detection, response, and reporting elements. In this role, Ms. Suro also oversees the surveillance and investigations teams responsible for providing enterprise-wide coverage relating to financial and cyber fraud against clients as well as fraud and regulatory violations associated with Registered Investment Advisors (RIAs) using Schwab's Advisor Services platform. Prior to returning to Schwab in her current capacity in 2015, Ms. Suro was a Director with Schwab's Compliance Regulatory Group from 2011 to 2012. Ms. Suro has a JD and was previously a securities attorney with Bingham McCutchen.

Tina Tambiah is Senior Director in the National Cause and Financial Crimes Detection Programs. In this role, she oversees FINRA's centralized intake unit responsible for reviewing and investigating regulatory events, including investor complaints and regulatory tips. Prior to this role, Ms. Tambiah was an Investigations Director in the Retail Firm Grouping. She led a team managing large and complex investigations which included fraudulent activity and other serious misconduct. Prior to 2019, Ms. Tambiah held management roles in the Firm Exam and Cause programs while in the Boston District Office where she was responsible for managing routine and specialized examinations of member broker-dealers and investigations of

customer complaints, termination for cause, disclosure filings and regulatory tips against individual brokers. She has presented case findings and disciplinary action recommendations to the enforcement department for disciplinary action proceedings. Ms. Tambiah earned her Bachelor of Arts degree in Economics from Stony Brook University.

Left of Boom: Fraud Prevention Solutions

Panelists

- **Moderator**
  - Jamie Udinson, Senior Director, Strategic Alliances, FINRA Member Supervision
- **Panelists**
  - Jason Foye, Senior Director, Special Investigations Unit, FINRA Member Supervision
  - Ivy Gong, Global Head of Fraud Operations, Morgan Stanley
  - Kara Suro, Managing Director, Head of Fraud Risk Management, Charles Schwab & Co., Inc.
  - Tina Tambiah, Senior Director, Initial Review Group, FINRA Member Supervision

FEBRUARY 2022

2022 Report on FINRA's Examination and Risk Monitoring Program

Introduction

The 2022 Report on FINRA's Examination and Risk Monitoring Program (the Report) provides firms with information that may help inform their compliance programs. For each topical area covered, the Report identifies the relevant rule(s), highlights key considerations for member firms' compliance programs[1], summarizes noteworthy findings from recent examinations, outlines effective practices that FINRA observed during its oversight, and provides additional resources that may be helpful to member firms in reviewing their supervisory procedures and controls and fulfilling their compliance obligations.

FINRA's intent is that the Report be an up-to-date, evolving resource or library of information for firms. To that end, the Report builds on the structure and content in the 2021 Report by adding new topics (*e.g.,* Disclosure of Order Routing Information, Funding Portals) denoted **NEW FOR 2022** and new material (*e.g.,* new exam findings, effective practices) to existing sections where appropriate. (New material in existing sections is in **bold** type.) In addition, those general findings that are also particularly relevant for firms in their first year of operation are denoted with a star (★).

As always, FINRA welcomes feedback on how we can improve future publications of this Report. Please contact Steve Polansky, Senior Director, Member Supervision at (202) 728-8331 or by email; or Rory Hatfield, Associate Principal Research Analyst, Member Supervision at (240) 386-5487 or by email.

Selected Highlights

In 2021, considerable industry, and in some cases public, attention was focused on topics that FINRA also addressed through its exam and risk monitoring program. These topics include newer SEC Rules (*e.g.,* Regulation Best Interest (Reg BI), Form CRS, amendments to Rule 606), recent increases in the number and sophistication of cybersecurity threats, and the proliferation of securities trading through mobile apps.

Reg BI and Form CRS

During Reg BI's and Form CRS' first full calendar year of implementation in 2021, FINRA expanded the scope of its reviews and testing relative to 2020 to execute a more comprehensive review of firms' processes, practices and conduct in areas such as establishing and enforcing adequate written supervisory procedures (WSPs); filing, delivering and tracking accurate Forms CRS; making

recommendations that adhere with Reg BI's Care Obligation; identifying and mitigating conflicts of interest; and providing effective training to staff. In this Report, FINRA notes its initial findings from its Reg BI and Form CRS reviews during the past year and will share additional findings at a future date.

CAT

FINRA continues to evaluate member firms that receive or originate orders in National Market System (NMS) stocks, over-the-counter (OTC) equity securities and listed options for compliance with Securities Exchange Act of 1934 (Exchange Act) Rule 613 and the CAT NMS Plan FINRA Rule 6800 Series (Consolidated Audit Trail Compliance Rule) (collectively, CAT Rules). This year's Report addresses compliance with certain CAT obligations, such as reporting CAT information to the Central Repository and maintaining an effective supervision process (including clock synchronization performed by third-party vendors).

Order Handling, Best Execution and Conflicts of Interest

Assessing firms' compliance with their best execution obligations under FINRA Rule 5310 (Best Execution and Interpositioning) is one of the cornerstones of FINRA's oversight activities. This oversight has evolved with changes in firms' business models, for example the advent of the "zero commission" model.

As noted in last year's Report, FINRA launched a targeted exam to "evaluate the impact that not charging commissions has or will have on the member firms' order-routing practices and decisions, and other aspects of member firms' business." FINRA will share its findings with member firms at a future date.

In addition, FINRA is focusing on firms' compliance with Rule 606 of Regulation NMS, which requires broker-dealers to disclose information regarding the handling of their customers' orders in NMS stocks and listed options. This information provides transparency to customers and can help them: better understand how their firm routes and handles their orders; assess the quality of order handling services provided by their firm; and determine whether their firm is effectively managing potential conflicts of interest that may impact their firm's routing decisions.

Mobile Apps

Advances in technology and its application continue to reshape the way some firms attract and interact with customers on mobile apps. These innovations can benefit investors in several ways, including increasing their market participation, expanding the types of products available to them and educating them on financial concepts. At the same time, however, these apps raise novel questions and potential concerns, such as whether they encourage retail investors to engage in trading activities and strategies that may not be consistent with their investment goals or risk tolerance, and how the apps' interface designs could influence investor behavior.

FINRA has identified significant problems with some mobile apps' communications with customers and firms' supervision of activity on those apps (particularly controls around account openings). FINRA has also observed mobile apps making use of social media to acquire customers, and recently initiated a targeted exam to assess firms' practices in this area, including with respect to firms' management of their obligations related to information collected from those customers and other individuals who may provide data to firms; FINRA will share its findings from this review after its completion.

Special Purpose Acquisition Companies (SPACs)

Another topic that has received significant attention is the increased use of Special Purpose Acquisition Companies (SPACs) to bring companies public. For example, in 2019, approximately 25 percent of initial public offerings were accomplished through SPACs; in the first quarter of 2021, this figure was over 70 percent.

FINRA recognizes how SPACs can provide companies with access to diverse funding mechanisms and allow investors to access new investment opportunities; however, as SPAC activity has increased, so too has FINRA's focus on broker-dealers' compliance with their regulatory obligations in executing SPAC transactions. In October 2021, FINRA launched a targeted exam to explore a range of issues, including how firms manage potential conflicts of interest in SPACs, whether firms are performing adequate due diligence on merger targets and if firms are providing adequate disclosures to customers. At a future date, FINRA will share with member firms its findings from this review.

Cybersecurity

Cybersecurity threats are one of the primary risks firms and their customers face. Over the past year, FINRA has continued to observe increases in the number and sophistication of these threats. For example, in 2021, FINRA has alerted firms about phishing campaigns involving fraudulent emails purporting to be from FINRA, as well as new customers opening online brokerage accounts to engage in Automated Clearing House (ACH) "instant funds" abuse. FINRA has issued additional regulatory guidance concerning the increase of bad actors using compromised registered representative or employee email accounts to execute transactions or move money; using customer information to gain unauthorized entry to customers' email accounts, online brokerage accounts or both (*i.e.,* customer account takeover (ATO) incidents); and using synthetic identities to fraudulently open new accounts. FINRA will continue to assess firms' programs to protect sensitive customer and firm information, as well as share effective practices firms can employ to protect their customers and themselves. Where appropriate, FINRA will also share information about cybersecurity threats to firms.

Complex Products

FINRA will continue to review firms' communications and disclosures made to customers in relation to complex products, and will review customer account activity to assess whether firms' recommendations regarding these products are in the best interest of the retail customer given their investment profile and the potential risks, rewards and costs associated with the recommendation. In addition, in August of last year, FINRA launched a targeted exam to review members' practices and controls related to the opening of options accounts which, in some instances, may be used to engage in complex strategies involving multiple options (such as spreads). FINRA will share its findings from this review at a future date.

How to Use This Report

FINRA's Risk Monitoring and Examination Programs evaluate member firms for compliance with relevant obligations and consider specific risks relating to each firm, including those relating to a firm's business model, supervisory control system and prior exam findings, among other considerations. While the topics addressed in this Report are selected for their interest to the largest number of member firms, they may include areas that are not relevant to an individual member firm and omit other areas that are applicable.

FINRA advises each member firm to review the Report and consider incorporating relevant practices into its compliance program in a manner tailored to its activities. The Report is intended to be just one of the tools a member firm can use to help inform the development and operation of its compliance program; it does not represent a complete inventory of regulatory obligations, compliance considerations, examination findings, effective practices or topics that FINRA will examine.

FINRA also reminds member firms to stay apprised of new or amended laws, rules and regulations, and to update their WSPs and compliance programs on an ongoing basis, as new regulatory obligations may be part of future examinations. FINRA encourages member firms to reach out to their designated Risk Monitoring Analyst if they have any questions about the considerations, findings and effective practices described in this Report.

Each area of regulatory obligations is set forth as follows:

- **Regulatory Obligations and Related Considerations** – A brief description of:
  - relevant federal securities laws, regulations and FINRA rules; and
  - questions FINRA may ask or consider when examining your firm for compliance with such obligations.

- **Exam Findings and Effective Practices**
  - Noteworthy findings that FINRA has noted at some—but not all—member firms, including:
    - new findings from recent examinations;
    - findings we highlighted in prior Reports and that we continue to note in recent examinations;
    - in certain sections, topics noted as "Emerging Risks" representing potentially concerning practices that FINRA has observed and which may receive increased scrutiny going forward; and
    - for certain topics—such as Cybersecurity, Liquidity Management and Credit Risk—observations that suggested improvements to a firm's control environment to address potential weaknesses that elevate risk, but for which there are not specific rule violations.
  - Select effective practices FINRA observed in recent exams, as well as those we noted in prior Exam Findings Reports and which we continue to see, that may help member firms, depending on their business model, evaluate their own programs.

- **Additional Resources** – A list of relevant FINRA Notices, other reports, tools and online resources.

The Report also includes an Appendix that outlines how member firms have used similar FINRA reports (*e.g.,* Exam Findings Reports, Priorities Letters) in their compliance programs.

As a reminder, the Report—like our previous Exam Findings Reports and Priorities Letters—does not create any new legal or regulatory requirements or new interpretations of existing requirements. You should not infer that FINRA requires member firms to implement any specific practices described in this report that extend beyond the requirements of existing federal securities provisions or FINRA rules.

Firm Operations

Anti-Money Laundering

Regulatory Obligations and Related Considerations

Regulatory Obligations:

The Bank Secrecy Act (BSA) and implementing regulations form the foundation for member firms' Anti-Money Laundering (AML) obligations. (The BSA has been amended several times, including by the USA PATRIOT ACT of 2001 and the Anti-Money Laundering Act of 2020.) **The implementing regulations impose a number of requirements on broker-dealers, which include implementing and maintaining both AML programs and Customer Identification Programs (CIPs); filing reports of suspicious activity; verifying the identity of legal entity customers; maintaining procedures for conducting ongoing customer due diligence; establishing due diligence programs to assess the money laundering risk presented by correspondent accounts maintained for foreign financial institutions; and responding to information requests from the Financial Crimes Enforcement Network (FinCEN) within specified timeframes.**

FINRA Rule 3310 (Anti-Money Laundering Compliance Program) requires that members develop and implement a written AML program reasonably designed to comply with the requirements of the BSA and its implementing regulations. **FINRA Rule 3310 also requires FINRA member firms to, among other things, establish and implement policies, procedures and internal controls that can be reasonably expected to detect and cause the reporting of suspicious activity; provide for an independent test of the AML program each calendar year (or every two years in some specialized cases); and provide ongoing training for appropriate personnel.**

Related Considerations:

- Does your firm's AML program reasonably address your business model, new and existing business lines, products, customers, geographic locations and associated AML risks?
- **Has your firm experienced substantial growth or changes to its business? If so, has its AML program reasonably grown and evolved alongside the business?**
- **Do your firm's AML procedures recognize that the suspicious activity reporting obligation may apply to any transactions conducted by, at or through the firm, even transactions that do not originate with your firm's customers?**
- **Does your firm have appropriately designed AML procedures to identify and respond to known indicators of suspicious activity involving low-priced securities, such as those detailed in FINRA *Regulatory Notices* *19-18* and *21-03*?**
- Does your firm's independent AML testing confirm that it maintains and implements reasonably designed procedures for suspicious activity detection and reporting?
- Does your firm collect identifying information and verify the identity of all individuals and entities that would be considered customers under the CIP Rule, and beneficial owners of legal entity customers under the Customer Due Diligence (CDD) Rule?
- **If your firm uses automated surveillance systems for suspicious activity monitoring, does your firm review the integrity of its data feeds and assess scenario parameters as needed?**
- If your firm introduces customers and activity to a clearing firm, how does your firm coordinate with your clearing firm, including with respect to the filing of Suspicious Activity Reports (SARs)?

- **Has your firm established and implemented appropriate procedures to: communicate cyber events to its AML department, Compliance department or both; fulfill regulatory obligations, such as the filing of SARs; and inform reviews of potentially impacted customer accounts?**
- **Has your firm reviewed FinCEN's first government-wide priorities for AML and countering the financing of terrorism (AML/CFT) policy ("AML/CFT Priorities"), and considered how the AML/CFT Priorities will be incorporated into its risk-based AML program?**

Emerging Low-Priced Securities Risk

FINRA has observed an increase in several types of activity in low-priced securities that could be indicative of fraud schemes—including an increase in such activity through foreign financial institutions (FFIs) that open omnibus accounts at U.S. broker-dealers. Recent trends indicate that FFIs may be "nesting"[2] within omnibus accounts of financial institutions based in jurisdictions that are generally considered to be lower risk, such as Canada or the United Kingdom.

To assist member firms in detecting and preventing these schemes—as well as mitigating the harm they cause to investors and the market—FINRA is sharing some of the signs of potentially illicit trading activity in low-priced securities that it has recently observed, which include:

- trading that coincides with a sudden increase in share price or trading volume, in the absence of legitimate news surrounding the company;
- investors depositing large blocks of shares of low-priced securities originating from convertible debt acquired from the issuer or a third party, immediately selling the shares and then transferring the proceeds out of the account;
- transactions in securities of issuers making questionable claims regarding their products or services related to a recent, major event (*e.g.,* the COVID-19 pandemic) or a new trend (*e.g.,* cryptocurrency or non-fungible tokens (NFTs)) or both; and
- increased trading that overlaps with a surge in relevant promotional activity on social media, investor chat rooms and message boards.

Firms can find additional resources concerning potential warning signs of fraudulent activity:

- FINRA's Investor Alerts and Investor Insights webpages
- *Regulatory Notice 21-03* (FINRA Urges Firms to Review Their Policies and Procedures Relating to Red Flags of Potential Securities Fraud Involving Low-Priced Securities)
- *Regulatory Notice 19-18* (FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations)
- SEC's Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities
- SEC's Risk Alert on Compliance Issues Related to Suspicious Activity Monitoring and Reporting at Broker-Dealers

Exam Findings and Effective Practices

Exam Findings:

- **Inadequate Ongoing Monitoring and Reporting of Suspicious Transactions – Failing to establish and implement an AML program reasonably expected to detect and report suspicious activity in compliance with FINRA Rule 3310(a) by, for example:**
  - **not using AML reports or systems that accurately and reasonably capture potentially suspicious activity, and are free of data integrity issues;**
  - **not conducting and accurately documenting AML surveillance reviews;**
  - **not implementing appropriate risk-based procedures to understand the nature and purpose of customer relationships in order to develop a customer risk profile;**
  - **not implementing procedures that are reasonably designed to investigate inquiries from clearing firms that concern "red flags" of potentially suspicious activity;**
  - **not tailoring AML programs to risks presented by products, customers, business lines and transactions (*e.g.,* cash management products, low-priced securities trading) and wire and ACH transfers; and**
  - **not notifying AML departments of events that involve suspicious transactions (*e.g.,* cybersecurity events, account compromises or takeovers, new account fraud, fraudulent wires and ACH transfers).**
- **Inadequate AML Independent Tests – Failing to comply with FINRA Rule 3310(c) by conducting AML tests that fail to review key aspects of the AML program, are not performed within the required timeframe, are not completed by persons with the requisite independence or are not completed at all.**
- **Insufficient Compliance With Certain Requirements of the BSA – Failing to establish a risk-based CIP to verify the identity of each customer in compliance with FINRA Rule 3310(b), failing to verify the identity of the beneficial owners of legal entity customers in compliance with FINRA Rule 3310(f) or failing to conduct due diligence on correspondent accounts of foreign financial institutions in compliance with FINRA Rule 3310(b).**

Update on Initial Public Offerings (IPOs) of China-Based Issuers

FINRA has observed that some firms are underwriting IPOs and subsequent trading of issuers based in the People's Republic of China (China-based issuers), raising concerns that the investors in the IPOs may be serving as nominees for an undisclosed control person or persons. These IPOs are typically smaller in size (*i.e.,* less than $100 million) and listed on the lower qualification tiers of U.S. stock exchanges.

FINRA has observed red flags of potentially manipulative trading associated with how these investors open new accounts and trade these securities after the IPO is completed, including:

- numerous unrelated accounts being opened at the same time, including with similar banking information, physical addresses, email address domains and current employer (which is often associated with the IPO issuer);
- documents investors provide in order to open an account or verify source of funds that may have been altered or could be fictitious;
- wire transfers received into these accounts that exceed the financial wherewithal of the investor as indicated on their new account documents, exceed the value of the shares purchased in the IPO and are either sent from similar banks, or bank accounts that share certain identifying information (*e.g.,* employer of account holder, email domain);
- investor accounts being accessed by a different Internet Protocol (IP) or Media Access Control (MAC) address[3] than is known for the customer, granting log in and trading capabilities to a third party or both;
- multiple orders with substantial similar terms being placed at or around the same time by seemingly unrelated investors in the same security that is indicative of "spoofing" or "layering"; and
- investors engaging in trading activity that does not make economic sense.

Given the potential risks, firms underwriting these IPOs and whose customers trade in these securities after the IPO should carefully evaluate whether they have controls in place necessary to identify and report market manipulation, other abusive trading practices and potential AML concerns. Firms can find additional information regarding the risks associated with China-based issuers in recent statements from the SEC:

- Emerging Market Investments Entail Significant Disclosure, Financial Reporting and Other Risks; Remedies are Limited
- Disclosure Considerations for China-Based Issuers
- [Chairman Gensler's] Statement on Investor Protection Related to Recent Developments in China

Effective Practices:

- **Risk Assessments** – Conducting an initial, formal written risk assessment and updating it based on the results of AML tests, audits and changes in size or risk profile of the firm (*e.g.,* business lines, products and services, registered representatives and customers).
- **Verifying Customers' Identities When Establishing Online Accounts – In meeting their CIP obligations, validating identifying information or documents provided by applicants (*e.g.,* Social Security number (SSN), address, driver's license), including, for example, through "likeness checks"; asking follow-up questions or requesting additional documents based on information from credit bureaus and credit reporting agencies, or digital identity intelligence (*e.g.,* automobile and home purchases); contracting third-party vendors to provide additional support (*e.g.,* databases to help verify the legitimacy of suspicious information in customers' applications); limiting automated approval of multiple accounts**

by a single customer; reviewing account applications for repetition or commonalities amongst multiple applications; and using technology to detect indicators of automated scripted attacks.[4]

- **Delegation and Communication of AML Responsibilities – When AML programs rely on other business units to escalate red flags of suspicious activity, establishing clearly delineated written escalation procedures and recurring cross-department communication with AML and compliance staff.**
- **Training – In meeting their obligations to provide ongoing AML training for appropriate personnel under FINRA Rule 3310(e), establishing and maintaining AML training programs that are tailored for the respective roles and responsibilities of the AML department, as well as departments that regularly work with AML; that address regulatory and industry developments impacting AML risk or regulatory requirements; and that, where applicable, leverage trends and findings from quality assurance controls.**
- **Detection and Mitigation of Wire and ACH Fraud** – In meeting their obligations to conduct ongoing monitoring to identify and report suspicious transactions under FINRA Rule 3310(f), monitoring outbound money movement requests post-ACH setup and restricting fund transfers in certain situations (*e.g.,* identity theft is detected in an investor's account).[5]

Additional Resources

- SEC
  - **Risk Alert: Compliance Issues Related to Suspicious Activity Monitoring and Reporting**
  - **Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities**
- FinCEN
  - **Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic**
  - **Advisory on Cyber-Events and Cyber-Enabled Crime**
  - **Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments**
  - **Anti-Money Laundering and Countering the Financing of Terrorism National Priorities**
  - **Frequently Asked Questions (FAQs) regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through Suspicious Activity Reports (SARs)**
- FINRA
  - Anti-Money Laundering (AML) Topic Page, which includes:
    - Anti-Money Laundering (AML) Template for Small Firms
    - ***Regulatory Notice 21-36* (FINRA Encourages Firms to Consider How to Incorporate the Government-wide Anti-Money Laundering and Countering the Financing of Terrorism Priorities Into Their AML Programs)**
    - ***Regulatory Notice 21-18* (FINRA Shares Practices Firms Use to Protect Customers from Online Account Takeover Attempts)**
    - ***Regulatory Notice 21-03* (FINRA Urges Firms to Review Their Policies and Procedures Relating to Red Flags of Potential Securities Fraud Involving Low-Priced Securities)**
    - ***Regulatory Notice 20-32* (FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection with Potential Account Takeovers and New Account Fraud)**
    - *Regulatory Notice 20-13* (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)
    - *Regulatory Notice 19-18* (FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations)

FinCEN National AML/CFT Priorities

As noted in *Regulatory Notice* 21-36, on June 30, 2021, FinCEN issued the AML/CFT Priorities, which identify and describe the most significant AML/CFT threats currently facing the United States (*e.g.,* cybercrime, domestic and international terrorist financing, securities and investment fraud).

The publication of the AML/CFT Priorities does not create an immediate change in BSA requirements or supervisory expectations for member firms, and FINRA is not currently examining for the incorporation of the AML/CFT Priorities into member firms' AML programs. Nevertheless, in preparation for any new requirements when the final regulations are effective, broker-dealers may wish to start considering how they will incorporate the AML/CFT Priorities into their risk-based AML programs.

Cybersecurity and Technology Governance

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Rule 30 of the SEC's Regulation S-P requires firms to have written policies and procedures that are reasonably designed to safeguard customer records and information. FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) also applies to denials of service and other interruptions to members' operations. In addition to firms' compliance with SEC regulations, FINRA reminds firms that cybersecurity remains one of the principal operational risks facing broker-dealers and expects firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations.

Technology-related problems, such as problems in firms' change- and problem-management practices or issues related to an increase in trading volumes, can expose firms to operational failures that may compromise firms' ability to comply with a range of rules and regulations, including FINRA Rules 4370, 3110 (Supervision) and 4511 (General Requirements), as well as Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3 and 17a-4.

Related Considerations:

Cybersecurity

- **What is the firm's process for continuously assessing cybersecurity and technology risk?**
- What kind of governance processes has your firm developed to identify and respond to cybersecurity risks?
- What is the scope of your firm's Data Loss Prevention program, including encryption controls and scanning of outbound emails to identify sensitive information?
- How does your firm identify and address branch-specific cybersecurity risks?
- What kind of training does your firm conduct on cybersecurity, including phishing?
- What process does your firm have to evaluate your firm's vendors' cybersecurity controls?
- **What types of penetration ("PEN") testing, if any, does your firm do to test web-facing systems that allow access to customer information or trading?**
- **How does your firm monitor for imposter websites that may be impersonating your firm or your registered representatives? How does your firm address imposter websites once they are identified?**
- **What are your firm's procedures to communicate cyber events to AML or compliance staff related to meeting regulatory obligations, such as the filing of SARs and informing reviews of potentially impacted customer accounts?**

Cybercrime

- FINRA continues to observe fraudsters and other bad actors engaging in cybercrime that increases both fraud risk (*e.g.,* synthetic identity theft, customer account takeovers, illegal transfers of funds, phishing campaigns, imposter websites) and money laundering risk (*e.g.,* laundering illicit proceeds through the financial system).
- Events involving, or enabled by, cybercrime are expected to be reported via SARs. FINRA has also published *Regulatory Notice* 21-18 (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts), which discusses cybersecurity practices firms may find effective in mitigating risks related to ATOs and funds transfers.

Technology Governance

- What controls does your firm implement to mitigate system capacity performance and integrity issues that may undermine its ability to conduct business and operations, monitor risk or report key information?
- How does your firm document system change requests and approvals?
- What type of testing does your firm perform prior to system or application changes being moved into a production environment and post-implementation?
- What are your firm's procedures for tracking information technology problems and their remediation? Does your firm categorize problems based on their business impact?

Exam Findings and Effective Practices

Exam Findings:

- **Inadequate Risk Assessment Process – Not having an adequate and ongoing process to assess cyber and IT risks at the firm, including, for example, failing to test implemented controls or conducting PEN testing regularly.**
- **Data Loss Prevention Programs – Not encrypting all confidential data, including a broad range of non-public customer information in addition to Social Security numbers (such as other account profile information) and sensitive firm information.**
- **Branch Policies, Controls and Inspections** – Not maintaining branch-level written cybersecurity policies; inventories of branch-level data, software and hardware assets; and branch-level inspection and automated monitoring programs.
- **Training** – Not providing ongoing comprehensive training to registered representatives, other firm personnel, third-party providers and consultants on cybersecurity risks relevant to individuals' roles and responsibilities (*e.g.,* phishing).
- **Vendor Controls** – Not implementing and documenting formal policies and procedures to review prospective and existing vendors' cybersecurity controls and managing the lifecycle of firms' engagement with all vendors (*i.e.,* from onboarding, to ongoing monitoring, through off-boarding, including defining how vendors will dispose of non-public client information).

Emerging Vendor Risk

Due to the recent increase in the number and sophistication of cyberattacks during the COVID-19 pandemic, FINRA reminds firms of their obligations to oversee, monitor and supervise cybersecurity programs and controls provided by third-party vendors.

Firms can find guidance in this area in *Regulatory Notice* 21-29 (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors) and the Cybersecurity and Infrastructure Security Agency's (CISA) Risk Considerations for Managed Service Provider Customers.

- **Access Management** – Not implementing access controls, including developing a "policy of least privilege" to grant system and data access only when required and removing it when no longer needed; not limiting and tracking individuals with administrator access; and not implementing multi-factor authentication (MFA) for registered representatives, employees, vendors and contractors.
- **Inadequate Change Management Supervision** – Insufficient supervisory oversight for application and technology changes (including upgrades, modifications to or integration of firm or vendor systems), which lead to violations of other regulatory obligations, such as those relating to data integrity, cybersecurity, books and records, and confirmations.
- **Limited Testing and System Capacity** – Order management system, online account access and trading algorithm malfunctions due to a lack of testing for changes or system capacity issues.

Effective Practices:

- **Insider Threat and Risk Management** – Collaborating across technology, risk, compliance, fraud and internal investigations/conduct departments to assess key risk areas, monitor access and entitlements, and investigate potential violations of firm rules or policies regarding data access or data accumulation.
- **Incident Response Planning** – Establishing and regularly testing (often using tabletop exercises) a written formal incident response plan that outlines procedures for responding to cybersecurity and information security incidents; and developing frameworks to identify, classify, prioritize, track and close cybersecurity-related incidents.
- **System Patching** – Implementing timely application of system security patches to critical firm resources (*e.g.,* servers, network routers, desktops, laptops, mobile phones, software systems) to protect non-public client or firm information.
- **Asset Inventory** – Creating and keeping current an inventory of critical information technology assets—including hardware, software and data—as well as corresponding cybersecurity controls.
- **Change Management Processes** – Implementing change management procedures to document, review, prioritize, test, approve, and manage internal and third-party hardware and software changes, as well as system capacity, in order to protect non-public information and firm services.
- **Online System Capacity – Continuously monitor and test the capacity of current systems, and track average and peak utilization, to anticipate the need for additional resources based on increases in accounts or trading volumes, as well as changes in systems.**
- **Customer Account Access – Requiring customers to use MFA to access their online accounts.**

Additional Resources

FINRA's Cybersecurity Topic Page, including:

- ***Regulatory Notice 21-29* (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors)**
- ***Regulatory Notice 21-18* (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts)**
- *Regulatory Notice 20-32* (FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud)
- ***Regulatory Notice 20-30* (Fraudsters Using Registered Representatives Names to Establish Imposter Websites)**
- *Information Notice 03/26/20* (Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19))
- *Regulatory Notice 20-13* (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)
- Report on Selected Cybersecurity Practices – 2018
- Report on Cybersecurity Practices – 2015
- Small Firm Cybersecurity Checklist
- Core Cybersecurity Controls for Small Firms
- Firm Checklist for Compromised Accounts
- Customer Information Protection Topic Page
- Cross-Market Options Supervision: Potential Intrusions Report Card
- Non-FINRA Cybersecurity Resources

Outside Business Activities and Private Securities Transactions

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA Rules 3270 (Outside Business Activities of Registered Persons) and 3280 (Private Securities Transactions of an Associated Person) require registered representatives to notify their firms in writing of proposed outside business activities (OBAs), and all associated persons to notify their firms in writing of proposed private securities transactions (PSTs), so firms can determine whether to limit or allow those activities. A firm approving a PST where the associated person has or may receive selling compensation must record and supervise the transaction as if it were executed on behalf of the firm.

Related Considerations:

- What methods does your firm use to identify individuals involved in undisclosed OBAs and PSTs?
- Do your firm's WSPs explicitly state when notification or pre-approval is required to engage in an OBA or PST?
- Does your firm require associated persons or registered persons to complete and update, as needed, questionnaires and attestations regarding their involvement— or potential involvement—in OBAs and PSTs; and if yes, how often?

- **Upon receipt of a written notice of proposed OBAs, does your firm consider whether they will interfere with or otherwise compromise the registered person's responsibilities to the firm and the firm's customers, be viewed by customers or the public as part of the member's business or both? Does your firm also determine whether such activities should be treated as a PST (subject to the requirements of FINRA Rule 3280)?**
- Does your firm have a process in place to update a registered representative's Form U4 with activities that meet the disclosure requirements of that form?
- Does your firm take into account the unique regulatory considerations and characteristics of digital assets when reviewing digital asset OBAs and PSTs?
- Does your firm record PSTs for compensation on its books and records, including PSTs involving new or unique products and services?
- How does your firm supervise activities that are PSTs, including digital asset PSTs, and document its compliance with the supervisory obligations?

Exam Findings and Effective Practices

Exam Findings:

- **Incorrect Interpretation of Compensation** – Interpreting "compensation" too narrowly (by focusing on only direct compensation, such as salary or commissions, rather than evaluating all direct and indirect financial benefits from PSTs, such as membership interests, receipt of preferred securities and tax benefits); and as a result, erroneously determining that certain activities were not PSTs.
- **Inadequate Consideration of Need to Supervise** – Approving participation in proposed transactions without adequately considering whether the firms need to supervise the transaction as if it were executed on their own behalf.
- **No Documentation** – Not retaining the documentation necessary to demonstrate the firm's compliance with the supervisory obligations for PSTs and not recording the transactions on the firm's books and records because certain PSTs were not consistent with the firm's electronic systems (such as where securities businesses conducted by a registered representative would not be captured in their clearing firm's feed of purchases and sales activity).
- **No or Insufficient Notice and Notice Reviews** – Registered persons failing to notify their firms in writing of OBAs or PSTs; and WSPs not requiring the review of such notices, or the documentation that such reviews had taken place.
- **Inadequate Controls** – Inadequate controls to confirm adherence to limitations placed on OBAs or PSTs, such as prohibiting registered representatives from soliciting firm clients to participate in an OBA or PST.
- **No Review and Recordkeeping of Digital Asset Activities** – Failing to conduct the required assessment of OBAs that involve digital assets or incorrectly assuming all digital assets are not securities and therefore, not evaluating digital asset activities, including activities performed through affiliates, to determine whether they are more appropriately treated as PSTs; and for certain digital asset or other activities that were deemed to be PSTs for compensation, not supervising such activities or recording such transactions on the firm's books and records.

Effective Practices:

- **Questionnaires** – Requiring registered representatives and other associated persons to complete upon hire, and periodically thereafter, detailed, open-ended questionnaires with regular attestations regarding their involvement—or potential involvement—in new or previously disclosed OBAs and PSTs (including asking questions relating to any other businesses where they are owners or employees; whether they are raising money for any outside activity; whether they act as "finders" for issuers seeking new investors; and any expected revenues or other payments they receive from any entities other than the member firm, including affiliates).

- **Due Diligence** – Conducting due diligence to learn about all OBAs and PSTs at the time of a registered representative's initial disclosure to the firm and periodically thereafter, including interviewing the registered representative and thoroughly reviewing:
  - social media, professional networking and other publicly available websites, and other sources (such as legal research databases and court records);
  - email and other communications;
  - documentation supporting the activity (such as organizational documents); and
  - **OBAs that involve raising capital or directing securities transactions with investment advisers or fund companies in order to identify potential PSTs.** ★
- **Monitoring** – Monitoring significant changes in, or other red flags relating to, registered representatives' or associated persons' performance, production levels or lifestyle that may indicate involvement in undisclosed or prohibited OBAs and PSTs (or other business or financial arrangements with their customers, such as borrowing or lending), including conducting regular, periodic background checks and reviews of:
  - correspondence (including social media);
  - fund movements;
  - marketing materials;
  - online activities;
  - customer complaints; and
  - financial records (including bank statements and tax returns).
- **Affiliate Activities** – Considering whether registered representatives' and other associated persons' activities with affiliates, especially self-offerings, may implicate FINRA Rules 3270 and 3280.
- **WSPs** – Clearly identifying types of activities or investments that would constitute an OBA or PST subject to disclosure/approval or not, as well as defining selling compensation and in some cases providing FAQs to remind employees of scenarios that they might not otherwise consider to implicate these rules.
- **Training** – Conducting training on OBAs and PSTs during registered person and associated person onboarding and periodically thereafter, including regular reminders of written notice requirements and for registered persons to update their disclosures.
- **Disciplinary Action** – Imposing significant consequences—including heightened supervision, fines or termination—for persons who fail to notify firms in writing of their OBAs and PSTs, or fail to receive approval of their PSTs for compensation.
- **Digital Asset Checklists** – Creating checklists with a list of considerations to confirm whether digital asset activities would be considered OBAs or PSTs (including reviewing private placement memoranda or other materials and analyzing the underlying products and investment vehicle structures).

Additional Resources

- *Regulatory Notice* 21-25 (FINRA Continues to Encourage Firms to Notify FINRA if They Engage in Activities Related to Digital Assets)
- *Regulatory Notice* 18-08 (FINRA Requests Comment on Proposed New Rule Governing Outside Business Activities and Private Securities Transactions)
- *Notice to Members* 96-33 (NASD Clarifies Rules Governing RRs/IAs)
- *Notice to Members* 94-44 (Board Approves Clarification on Applicability of Article III, Section 40 of Rules of Fair Practice to Investment Advisory Activities of Registered Representatives)

Books and Records

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Exchange Act Rules 17a-3 and 17a-4, as well as FINRA Rule 3110(b)(4) (Review of Correspondence and Internal Communications) and the FINRA 4510 Rule Series (Books and Records Requirements) (collectively, Books and Records Rules) require a firm to, among other things, create and preserve, in an easily accessible place, originals of all communications received and sent relating to its "business as such."[6]

Additionally, firms must file a Financial Notification when selecting or changing an archival service provider, and are reminded to document the review of correspondence and confirm that individuals are not conducting supervisory reviews of their own correspondence. ★

Related Considerations:

- What kind of vendors, such as cloud service providers (Cloud Vendors), does your firm use to comply with Books and Records Rules requirements, including storing required records on electronic storage media (ESM)? How does it confirm compliance with the Books and Records Rules, ESM Standards and ESM Notification Requirements?
- Has your firm reviewed its Books and Records Rules policies and procedures to confirm they address all vendors, including Cloud Vendors?
- **If your firm emails its clients and customers links to Virtual Data Rooms (VDRs)—online data repositories that secure and distribute confidential information—does the firm retain and store documents embedded in those links once the VDRs are closed?**

Exam Findings and Effective Practices

Exam Findings:

- **Misinterpreted Obligations** – Not performing due diligence to verify vendors' ability to comply with Books and Records Rules requirements if they use that vendor; or not confirming that service contracts and agreements comply with ESM Notification Requirements because firms did not understand that all required records must comply with the Books and Records Rules, including records stored using Cloud Vendors' storage services.
- **No ESM Notification** – Not complying with the ESM Notification Requirements, including obtaining the third-party attestation letters required by Exchange Act Rule 17a-4(f)(3)(vii).

Effective Practices:

- **Contract Review** – Reviewing vendors' contracts and agreements to assess whether firms will be able to comply with the Books and Records Rules, ESM Standards and ESM Notification Requirements.
- **Testing and Verification** – Testing all vendors'—including Cloud Vendors'—capabilities to fulfill regulatory obligations by, for example, simulating a regulator's examinations by requesting records and engaging regulatory or compliance consultants to confirm compliance with the Books and Records Rules, ESM Standards and ESM Notification Requirements (and in some cases engaging the consultant to provide the third-party attestation).
- **Attestation Verification** – Confirming with vendors, including Cloud Vendors, whether the vendors will provide the third-party attestation.

Additional Resources

- Frequently Asked Questions about the 2001 Amendments to Broker-Dealer Books and Records Rules Under the Securities Exchange Act of 1934
- Books and Records Requirements Checklist
- Books and Records Topic Page

Direct Mutual Fund Business Risk

FINRA observed that some firms did not adequately supervise their direct mutual fund business (*i.e.,* selling mutual fund shares via "check and app" that are held directly by the mutual fund companies) because, for example, they were:

- maintaining blotters that did not include sufficient information to adequately supervise direct mutual fund transactions (*e.g.,* not all transactions are captured or key information is missing, such as customer name, fund symbol and share class);
- miscoding new mutual fund transactions as reinvestments or recurring contributions, which prevented them from going through firms' surveillance and supervision systems; and
- relying on *ad hoc* supervisory reviews by an insufficient number of designated principals.

As a result of these arrangements, many firms were unaware of, or had inadequate information about, direct mutual fund transactions that their registered representatives recommended or processed, and were not able to supervise them adequately. In some cases, this inability to supervise direct mutual fund business effectively resulted in firms not being able to identify inappropriate sales charge discounts, unsuitable share class recommendations and short-term mutual fund switching.

As part of their obligations under FINRA Rules 2010 (Standards of Commercial Honor and Principles of Trade), 2110 (Recommendations), 3110 (Supervision) and Reg BI, firms must supervise all activity of their registered representatives related to direct mutual fund transactions. Additionally, Exchange Act Rules 17a-3 and 17a-4 require firms to maintain and keep current purchase and sale blotters that contain relevant information for all direct mutual fund transactions, including redemptions. When evaluating your firm's supervision of its direct mutual fund business, consider these questions:

- What portion of your firm's mutual fund business is application-based directly with mutual fund companies (in terms of dollar volume and number of accounts)?
- How do your firm's policies and procedures address supervision of your firm's direct mutual fund business? What processes (*e.g.,* regularly reviewing exception reports) does your firm use to review direct mutual fund transactions for compliance with applicable FINRA rules and securities regulations? Are such policies and procedures reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules?
- What information does your firm gather from mutual fund companies or clearing entities (*e.g.,* National Securities Clearing Corporation, Depository Trust and Clearing Corporation) to support its ability to adequately supervise its direct mutual fund business?

For additional guidance, please refer to *Regulatory Notice 21-07* (FINRA Provides Guidance on Common Sales Charge Discounts and Waivers for Investment Company Products).

Regulatory Events Reporting

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA Rule 4530 (Reporting Requirements) requires firms to promptly report to FINRA, and associated persons to promptly report to firms, specified events, including, for example, violations of securities laws and FINRA rules, certain written customer complaints and certain disciplinary actions taken by the firm. Firms must also report quarterly to FINRA statistical and summary information regarding certain written customer complaints.

Related Considerations:

- Does your firm provide periodic reminders or training on such requirements, and what consequences does your firm impose on those persons who do not comply?
- How does your firm monitor for red flags of unreported written customer complaints and other reportable events?
- How does your firm confirm that it accurately and timely reports to FINRA written customer complaints that associated persons reported to your firm's compliance department?
- How does your firm determine the problem and product codes it uses for its statistical reporting of written customer complaints to FINRA?

Exam Findings and Effective Practices

Exam Findings:

- **No Reporting to the Firm** – Associated persons not reporting written customer complaints, judgments concerning securities, commodities- or financial-related civil litigation and other events to the firms' compliance departments because they were not aware of firm requirements.
- **Inadequate Surveillance** – Firms not conducting regular email and other surveillance for unreported events.
- **No Reporting to FINRA** – Failing to report to FINRA written customer complaints that associated persons reported to the firms' compliance departments.
- **Incorrect Rule 4530 Product/Problem Codes** – As part of the statistical reporting to FINRA, failing to use codes that correlated to the most prominent product or the most egregious problem alleged in the written customer complaints, but instead reporting less prominent or severe codes or other codes based on the firms' investigations or other information.

Effective Practices:

- **Compliance Questionnaires** – Developing detailed annual compliance questionnaires to verify the accuracy of associated persons' disclosures, including follow-up questions (such as whether they are the subject of any pending lawsuits or have received any written customer complaints).
- **Email Surveillance** – Conducting email surveillance targeted to identify unreported written customer complaints (by, for example, including complaint-related words in their keyword lexicons, reviewing for unknown email addresses and conducting random email checks).
- **Review of Registered Representatives' Financial Condition** – Identifying expenses, settlements and other payments that may indicate unreported events by conducting periodic reviews of their associated persons' financial condition, including background checks and credit reports.
- **Review of Publicly Available Information** – Conducting periodic searches of associated persons' names on web forums, court filings and other publicly available databases, including reviewing for any judgments concerning securities, commodities- or financial-related civil litigation and other reportable events.

Additional Resources

- *Regulatory Notice* 20-17 (FINRA Revises Rule 4530 Problem Codes for Reporting Customer Complaints and for Filing Documents Online)
- *Regulatory Notice* 20-02 (FINRA Requests Comment on the Effectiveness and Efficiency of Its Reporting Requirements Rule)
- *Regulatory Notice* 13-08 (FINRA Amends Rule 4530 to Eliminate Duplicative Reporting and Provide the Option to File Required Documents Online Using a New Form)
- FINRA's Rule 4530 Reporting Requirements
- FINRA's Rule 4530 Reporting Codes
- FINRA Report Center – 4530 Disclosure Timeliness Report Card

Firm Short Positions and Fails-to-Receive in Municipal Securities NEW FOR 2022

Regulatory Obligations and Related Considerations

Regulatory Obligations:

As detailed in *Regulatory Notice* 15-27, customers may receive taxable, substitute interest instead of the tax-exempt interest they were expecting when a firm effects sales to customers of municipal securities that are not under the firm's possession or control.[7] This can occur when firm trading activity inadvertently results in a short position or a firm fails to receive municipal securities it purchases to fulfill a customer's order.

Firms must develop and implement adequate controls and procedures for detecting, resolving and preventing these adverse tax consequences to customers. Such procedures must include closing out fails-to-receive within the time frame prescribed within Municipal Securities Rulemaking Board (MSRB) Rule G-12(h) and confirming that their communications with customers regarding the tax status of paid or accrued interest for municipal securities are neither false nor misleading, in accordance with MSRB Rule G-17.

Related Considerations:

- Does your firm use exception reports to manage its municipal securities' short positions or fails-to-receive? If so, how does your firm use such reports, and which departments are responsible for managing them?
- When municipal securities short positions are identified, does your firm begin to cover the shorts, or do they wait until the trades have settled?
- What is your firm's process to close out fails-to-receive in accordance with the methods and time frame prescribed under MSRB G-12(h)?
- How does your firm detect instances that would require them to pay customers substitute interest? In those circumstances, what is the firm's process for notifying impacted customers and paying them substitute interest in a timely manner? If a customer does not want to receive substitute interest, what alternatives does the firm offer (*e.g.,* offering to cancel the transaction and purchasing a comparable security that would provide tax-exempt interest)?
- How does your firm handle inbound or outbound account transfers sent through the Automated Customer Account Transfer Service (ACAT) that are delivered with no corresponding municipal bonds in possession or control?

Exam Findings and Effective Practices

Exam Findings:

- **Inadequate Controls and Procedures** – Not maintaining adequate procedures and controls for preventing, identifying and resolving adverse consequences to customers when a firm does not maintain possession or control of municipal securities that a customer owns.
- **Inadequate Lottery Systems** – Opting to use a random lottery system to allocate municipal short positions to certain customer accounts, but the system did not fairly or adequately account for or allocate substitute accrued interest payments.

Effective Practices:

- **Preventative Controls** – Maintaining processes to prevent or timely remediate municipal positions from settling short (*e.g.,* covering these positions, finding a suitable alternative, cancelling the customer's purchase).
- **Operational and Supervisory Reports** – Developing operational and supervisory reports to identify customer long positions for which the firm has not taken possession and control of the security.
- **Review of Fail Reports** – Municipal securities principals performing regular, periodic reviews of Fail Reports to comply with the close-out requirements of MSRB Rule G12-(h).

Additional Resource

- *Regulatory Notice* 15-27 (Guidance Relating to Firm Short Positions and Fails-to-Receive in Municipal Securities)

Trusted Contact Persons NEW FOR 2022

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA Rule 4512(a)(1)(F) (Customer Account Information) requires firms, for each of their non-institutional customer accounts, to make a reasonable effort to obtain the name and contact information for a trusted contact person (TCP) age 18 or older. FINRA Rule 4512 also describes the circumstances in which firms and their associated persons are authorized to contact the TCP and disclose information about the customer account.

Related Considerations:

- Has your firm established an adequate supervisory system, including WSPs, related to seeking to obtain and using the names and contact information for TCPs?
- Does your firm educate registered representatives about the importance of collecting and using trusted contact information, where possible?

Exam Findings and Effective Practices

Exam Findings:

- **No Reasonable Attempt to Obtain TCP Information** – Not making a reasonable attempt to obtain the name and contact information of a TCP for all non-institutional customers (*e.g.,* seeking to obtain this information only from senior non-institutional customers, not requesting this information within firm's regularly scheduled 36-month customer account records update letter).

- **No Written Disclosures** – Not providing a written disclosure explaining the circumstances under which the firm may contact a TCP when seeking to obtain TCP information (*e.g.,* when a new non-institutional account is opened or when the firm updates an existing account's information (in accordance with FINRA Rule 4512(b))).

Effective Practices:

- **Training** – Conducting training, for both front office and back office staff, on the warning signs of potential: (1) customer exploitation; (2) diminished capacity; and (3) fraud perpetrated on the customer.
- **Emphasizing the Importance of TCP and Promoting Effective Practices** –
  - Emphasizing at the senior-management level on down the importance of collecting TCP information.
  - Using innovative practices, such as creating target goals for collecting TCP and internally publicizing results among branch offices or regions.
  - Promoting effective ways of asking for TCP information and seeking feedback from registered representatives and supervisors on techniques that they have successfully used that have not already been publicized across the organization.
  - Establishing a system that notifies registered representatives when accessing non-institutional customer accounts that do not have a TCP listed and reminds them to request that information from customers.
- **Senior Investor Specialists** – Establishing specialized groups or appointing individuals to handle situations involving elder abuse or diminished capacity; contact customers' TCPs—as well as Adult Protective Services, regulators and law enforcement, when necessary—and guiding the development of products and practices focused on senior customers.
- **Firm Outreach** – Hosting conferences or joining industry groups focused on protecting senior customers.

Additional Resources

- SEC's, NAASA's and FINRA's Investor Resources for Establishing a Trusted Contact
- FINRA's Frequently Asked Questions Regarding FINRA Rules Relating to Financial Exploitation of Senior Investors
- *Regulatory Notice* 20-34 (Proposed Amendments to FINRA Rule 2165 and Retrospective Rule Review Report)

Emerging Customer Account Information Risks

Effective February 15, 2021, FINRA Rule 3241 (Registered Person Being Named a Customer's Beneficiary or Holding a Position of Trust for a Customer) requires a registered person to decline being named a beneficiary of a customer's estate, executor or trustee, or to have a power of attorney for a customer unless certain conditions are met, including providing written notice to the firm and receiving approval. The rule requires the firm with which the registered person is associated, upon receiving required written notice from the registered person, to review and approve or disapprove the registered person assuming such status or acting in such capacity.

Registered persons face potential conflicts of interest when they are named a customer's beneficiary, executor or trustee, or hold a power of attorney for their customer. These conflicts of interest can take many forms and can include a registered person benefiting from the use of undue and inappropriate influence over important financial decisions to the detriment of a customer.

When assessing your firm's compliance with Rule 3241, consider these questions:

- Do your firm's policies and procedures establish criteria for determining whether to approve a registered person assuming either status or acting in either capacity?
- Does your firm perform a reasonable assessment of the risks created by a registered person being named a customer's beneficiary or holding a position of trust for a customer?
- If your member firm imposes conditions or limitations on its approval, does it reasonably supervise the registered person's compliance with the corresponding conditions or limitations?
- Does your firm have WSPs, and deliver training, reasonably designed to make registered persons aware of the obligations under the rule and the firm's related procedures?

Funding Portals and Crowdfunding Offerings NEW FOR 2022

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Title III of the Jumpstart Our Business Startups (JOBS) Act enacted in 2012 contains provisions relating to securities offered or sold through crowdfunding. The SEC's Regulation Crowdfunding and FINRA's corresponding set of Funding Portal Rules set forth the principal requirements that apply to funding portal members.

Funding portals must register with the SEC and become a member of FINRA. Broker-dealers contemplating engaging in the sale of securities in reliance on the crowdfunding exemptions must notify FINRA in accordance with FINRA Rule 4518 (Notification to FINRA in Connection with the JOBS Act).

Related Considerations:

- What steps is your firm taking to confirm all required issuer information, pursuant to Regulation Crowdfunding Rules 201 and 203(a), is publicly available on your firm's platform?
- Does your firm plan to undergo or has it already undergone an operational or structural change that impacts the capitalization of the firm, pursuant to Funding Portal Rule 110(a)(4)? Has your firm reviewed the membership rules to confirm a Continuing Membership Application (CMA) is not required?

Exam Findings and Effective Practices

Exam Findings:

- **Failure to Obtain Attestation** – Not obtaining the attestation required by Regulation Crowdfunding Rule 404 when using a third-party vendor to store the required records.
- **Missing Disclosures** – Offerings on the platform do not contain all required disclosures as codified in Regulation Crowdfunding, in particular:
  - names of officers and directors of the issuer, and the positions held by these individuals for the past three years;
  - descriptions of the purpose and intended use of proceeds, the process to complete the offering transaction or cancel an investment commitment, the ownership and capital structure, the material terms of any indebtedness of the issuer; and
  - financial statements, as required by Regulation Crowdfunding Rule 201(t).
- **Failure to Report Customer Complaints** – Not reporting written customer complaints, as required by FINRA Funding Portal Rule 300(c).
- **Untimely Required Filings** – Not making required filings in a timely manner—such as filing the funding portal's Statement of Gross Revenue by the deadline of March 1—and not filing updates or changes to contact information within 30 days of the change.
- **Not Filing CMAs** – Funding portals effecting changes in ownership without obtaining prior approval from FINRA, as required by Funding Portal Rule 110(a)(4).

Effective Practices:

- **Compliance Resources** – Developing annual compliance questionnaires to verify the accuracy of associated persons' disclosures, including follow-up questions (such as whether they have ever filed for bankruptcy, have any pending lawsuits, are subject to an unsatisfied judgments or liens or received any written customer complaints), as well as compliance checklists and schedules to confirm that required obligations are being met in a timely manner, such as providing all issuer disclosure requirements of Regulation Crowdfunding Rule 201.
- **Supervision** – Implementing supervisory review procedures tailored to funding portal communications requirements that, for example, clearly define permissible and prohibited communications and identify whether any contemplated structural or organizational changes necessitate the filing of a CMA.

Additional Resource

- FINRA's Funding Portals Topic Page

Communications and Sales

Reg BI and Form CRS

Regulatory Obligations and Related Considerations

Regulatory Obligations:

The SEC's Regulation Best Interest (Reg BI) establishes a "best interest" standard of conduct for broker-dealers and associated persons when they make recommendations to retail customers of any securities transaction or investment strategy involving securities, including account recommendations. **Pursuant to this standard, a broker-dealer and its associated persons must not put their financial or other interests ahead of the interests of a retail customer.**

In addition, whether or not they make recommendations, firms that offer services to retail investors must provide them with a Form CRS, a brief relationship summary that discloses material information in plain language (*e.g.,* investment services provided, fees, conflicts of interest, legal and disciplinary history of the firms and financial professionals).

Reg BI and Form CRS became effective on June 30, 2020, and 2021 marked the first full calendar year during which FINRA examined firms' implementation of related obligations. The findings presented here are thus an initial look at firms' practices. FINRA will share further findings as we continue to conduct exams and gather additional information on firms' practices.

Related Considerations:

- **When your firm determines whether it is obligated to comply with Reg BI, does your firm consider the following key definitions in the context of the rule?**
  - **"Retail customer" is defined as "a natural person, or the legal representative of such natural person, who:**
    - **receives a recommendation of any securities transaction or investment strategy involving securities from a broker-dealer; and**
    - **uses the recommendation primarily for personal, family, or household purposes."**
  - **A retail customer "uses" a recommendation of a securities transaction or investment strategy involving securities when, as a result of the recommendation[8]:**
    - **the retail customer opens a brokerage account with the broker-dealer, regardless of whether the broker-dealer receives compensation;**
    - **the retail customer has an existing account with the broker-dealer and receives a recommendation from the broker-dealer, regardless of whether the broker-dealer receives or will receive compensation, directly or indirectly, as a result of that recommendation[9]; or**
    - **the broker-dealer receives or will receive compensation, directly or indirectly as a result of that recommendation, even if that retail customer does not have an account at the firm.**
- **Do your firm and your associated persons adhere to the Care Obligation of Reg BI when making recommendations by:**
  - **exercising reasonable diligence, care and skill to understand the potential risks, rewards and costs associated with a recommendation and having a reasonable basis to believe, based on that understanding, that the recommendation is in the best interest of at least some retail investors;**

  - **considering those risks, rewards and costs in light of the retail customer's investment profile and having a reasonable basis to believe that a recommendation is in that particular customer's best interest and does not place the broker-dealer's interest ahead of the customer's interest; and**
  - **having a reasonable basis to believe that a series of recommended transactions, even if in the retail customer's best interest when viewed in isolation, is not excessive and is in the retail customer's best interest when taken together in light of the retail customer's investment profile?**
- **Do your firm and your associated persons consider costs and reasonably available alternatives when making recommendations to retail customers?**
- **Are your firm's policies and procedures reasonably designed to identify and disclose or eliminate conflicts, as well as to mitigate conflicts that create an incentive for an associated person of the firm to place his or her interests or the interest of the firm ahead of the retail customer's interest?**
- **How does your firm test its policies and procedures to determine if they are adequate and performing as expected?**
- Does your firm place any material limitations on the securities or investment strategies involving securities that may be recommended to a retail customer? If so, does your firm identify and disclose such limitations and prevent those limitations from causing the firm or its associated persons to make recommendations that place the firm's or associated person's interests ahead of the retail customer's interest?
- **Are your firm's policies and procedures reasonably designed to identify and eliminate sales contests, sales quotas, bonuses and non-cash compensation that are based on the sale of specific securities or specific types of securities within a limited period of time, or mitigate conflicts for those not required to be eliminated?**
- **Do your firm's disclosures include a full and fair disclosure of all material facts relating to the scope and terms of the firm's relationship with retail customers (*e.g.,* material fees and costs associated with transactions or accounts, material limitations involving securities recommendations) and all material facts relating to conflicts of interest that are associated with the recommendation?**
- **What controls does your firm have to assess whether disclosures are provided timely, and if provided electronically, in compliance with the SEC's electronic delivery guidance?**
- **Do your firm's policies and procedures address Reg BI, including new obligations that did not exist prior to Reg BI?**
- **Do your firm's policies and procedures: (1) identify specific individual(s) who are responsible for supervising compliance with Reg BI; (2) specify the supervisory steps and reviews appropriate supervisor(s) should take and their frequency; and (3) note how supervisory reviews should be documented?**
- If your firm is not dually registered as an investment adviser, commodity trading advisor, municipal advisor or advisor to a special entity, do the firm or any of its associated persons who are not dually registered use "adviser" or "advisor" in their name or title?
- **Does the firm provide dually-registered associated persons with adequate guidance on how to determine and disclose the capacity in which they are acting?**
- Has your firm provided adequate Reg BI training to its associated persons, including supervisory staff?
- **If your firm offers services to retail investors:**
  - **does it deliver Form CRS to each new or prospective customer who is a retail investor before the earliest of: (i) a recommendation of an account type, securities transaction or investment strategy involving securities; (ii) placing an order for the retail investor; or (iii) opening a brokerage account for the investor?**

- **for existing retail investor customers, does the firm deliver Form CRS before or at the time the firm: (i) opens a new account that is different from the retail customer's existing account; (ii) recommends that the retail customer roll over assets from a retirement account; or (iii) recommends or provides a new service or investment outside of a formal account (*e.g.,* variable annuities or a first-time purchase of a direct-sold mutual fund through a "check and application" process)?**
- **does it file a relationship summary with the SEC through the Central Registration Depository (CRD), if the firm is registered as a broker-dealer; through the Investment Adviser Registration Depository (IARD), if the firm is registered as an investment adviser; or both CRD and IARD, if the firm is a dual-registrant?**
- **does your firm have processes in place to update and file the amended Form CRS within 30 days whenever any information becomes materially inaccurate and to communicate, without charge, any changes in the updated relationship summary to retail investors who are existing customers within 60 days after the updates are required to be made (a total of 90 days to communicate the changes to customers after the information becomes materially inaccurate)?**

Exam Findings and Effective Practices

Exam Findings:

Reg BI and Form CRS

- **WSPs That Are Not Reasonably Designed To Achieve Compliance with Reg BI and Form CRS –**
  - **Providing insufficiently precise guidance by:**
    - **not identifying the specific individuals responsible for supervising compliance with Reg BI; and**
    - **stating the rule requirements, but failing to detail how the firm will comply with those requirements (*i.e.,* stating "what" but failing to address "how").**
  - **Failing to modify existing policies and procedures to reflect Reg BI's requirements by:**
    - **not addressing how costs and reasonably available alternatives should be considered when making recommendations;**
    - **not addressing recommendations of account types;**
    - **not addressing conflicts that create an incentive for associated persons to place their interest ahead of those of their customers; and**
    - **not including provisions to address Reg BI-related recordkeeping obligations and the testing of the firms' Reg BI and Form CRS policies, procedures and controls.**
  - **Failing to develop adequate controls or developing adequate controls but not memorializing these processes in their WSPs.**
- **Inadequate Staff Training – Failing to adequately prepare associated persons to comply with the requirements of Reg BI beyond previous suitability obligations or Form CRS by:**
  - **failing to deliver initial training before the June 30, 2020, compliance date;**
  - **delivering training without making clear Reg BI's new obligations; or**
  - **delivering training that focused on Reg BI and Form CRS requirements in general, without addressing the specific steps associated persons should take to comply with these requirements.**

- **Failure to Comply With Care Obligation –**
  - **Making recommendations that were not in the best interest of a particular retail customer based on that retail customer's investment profile and the potential risks, rewards and costs associated with the recommendation.**
  - **Recommending a series of transactions that were excessive in light of a retail customer's investment profile and placing the broker-dealer's or associated person's interest ahead of those of retail customers.**
- **Failure to Comply with Conflict of Interest Obligation – Not identifying conflicts or, if identified, not adequately addressing those conflicts.**
- **Improper Use of the Terms "Advisor" or "Adviser" – Associated persons, firms or both, using the terms "advisor" or "adviser" in their titles or firm names, even though they lack the appropriate registration.[10]**
- **Insufficient Reg BI Disclosures – Not providing retail customers with "full and fair" disclosures of all material facts related to the scope and terms of their relationship with these customers or related to conflicts of interest that are associated with the recommendation, including:**
  - **material fees received as a result of recommendations made (*e.g.,* revenue sharing or other payments received from product providers or issuers, as well as other fees tied to recommendations to rollover qualified accounts);**
  - **potential conflicts of interest (*e.g.,* associated persons trading in the same securities in their personal account(s) or outside employment); and**
  - **material limitations in securities offerings.**

Form CRS

- **Deficient Form CRS Filings – Firms' Form CRS filings significantly departing from the Form CRS instructions or guidance from the SEC's FAQ on Form CRS by:**
  - **exceeding prescribed page lengths;**
  - **omitting material facts (*e.g.,* description of services offered; limitations of the firm's investment services);**
  - **inaccurately representing their financial professionals' disciplinary histories;**
  - **failing to describe types of compensation and compensation-related conflicts;**
  - **incorrectly stating that the firm does not provide recommendations;**
  - **changing or excluding language required by Form CRS; and**
  - **not resembling a relationship summary, as required by Form CRS.[11]**
- **Form CRS Not Posted Properly on Website – For firms that have a public website, failing to post or failing to post prominently, in a location and format that is easily accessible to retail investors, the current Form CRS (*e.g.,* requiring multiple click-throughs or using confusing descriptions to navigate to the Form CRS).**
- **Inadequate Form CRS Amendments – Firms not in compliance with Form CRS in relation to material changes because they:**
  - **failed to re-file in CRD in a timely manner (*i.e.,* within 30 days of the date when Form CRS became materially inaccurate); or**

- **failed to communicate or timely communicate changes to existing retail investor customers (*e.g.,* delivering amended summary, with required exhibits, showing revised text or summarizing material changes or communicating the information through another disclosure within 60 days after the updates are required to be made—90 days total from the date when Form CRS became materially inaccurate).**

- **Misconstruing Obligation to File Form CRS –**
  - **Incorrectly determining that filing Form CRS hinges solely on making recommendations, rather than offering services to a retail investor.**
  - **Incorrectly claiming a firm is not subject to the Form CRS delivery obligation because of, among other things, their customer base (*e.g.,* retail investors who are high-net-worth individuals) or the services they offer (*e.g.,* investment company products held directly by an issuer, self-directed accounts)**

Effective Practices:

- **Identifying and Mitigating Conflicts of Interest – Identifying, disclosing, and eliminating or mitigating conflicts of interest across business lines, compensation arrangements, relationships or agreements with affiliates, and activities of their associated persons by:**
  - **establishing and implementing policies and procedures to identify and address conflicts of interest, such as through the use of conflicts committees or other mechanisms or creating conflicts matrices tailored to the specifics of the firm's business that address, for example, conflicts across business lines and how to eliminate, mitigate or disclose those conflicts;**
  - **sampling recommended transactions to evaluate how costs and reasonably available alternatives were considered;**
  - **providing resources to associated persons making recommendations that account for reasonably available alternatives with comparable performance, risk and return that may be available at a lower cost, such as:**
    - **worksheets, in paper or electronic form, to compare costs and reasonably available alternatives; or**
    - **guidance on relevant factors to consider when evaluating reasonably available alternatives to a recommended product (*e.g.,* similar investment types from the issuer; less complex or risky products available at the firm);**
  - **updating client relationship management (CRM) tools that automatically compare recommended products to reasonably available alternatives;**
  - **revising commission schedules within product types to flatten the percentage rate; and**
  - **broadly prohibiting all sales contests.**

- **Limiting High-Risk or Complex Investments for Retail Customers – Mitigating the risk of making recommendations that might not be in a retail customer's best interest by:**
  - **establishing product review processes to identify and categorize risk and complexity levels for existing and new products;**
  - **limiting high-risk or complex product, transaction or strategy recommendations to specific customer types; and**
  - **applying heightened supervision to recommendations of high-risk or complex products.**

- **Implementing Systems Enhancements for Tracking Delivery of Required Customer Documents – Tracking and delivering Form CRS and Reg BI-related documents to retail investors and retail customers in a timely manner by:**
  - **automating tracking mechanisms to determine who received Form CRS and other relevant disclosures; and**
  - **memorializing delivery of required disclosures at the earliest triggering event.**
- **Implementing New Surveillance Processes – Monitoring associated persons' compliance with Reg BI by:**
  - **conducting monthly reviews to confirm that their recommendations meet Care Obligation requirements, including system-driven alerts or trend criteria to identify:**
    - **account type or rollover recommendations that may be inconsistent with a customer's best interest;**
    - **excessive trading; and**
    - **sale of same product(s) to a high number of retail customers;**
  - **monitoring communication channels (*e.g.*, email, social media) to confirm that associated persons who were not investment adviser representatives (IARs) were not using the word "adviser" or "advisor" in their titles; and**
  - **incorporating Reg BI-specific reviews into the branch exam program as part of overall Reg BI compliance efforts, focusing on areas such as documenting Reg BI compliance and following the firms' Reg BI protocols.**

Additional Resources

- FINRA's SEC Regulation Best Interest Key Topics Page
- SEC's Regulation Best Interest Guidance Page
- SEC's Staff Statement Regarding Form CRS Disclosure
- 2021 FINRA Annual Conference: Regulation Best Interest and Form CRS: Recent Observations and What to Expect Panel
- 2021 Small Firm Virtual Conference: Regulation Best Interest and Form CRS Panel
- You may submit a question by email to IABDQuestions@sec.gov. Additionally, you may contact the SEC's Division of Trading and Markets' Office of Chief Counsel at (202) 551-5777.

Areas of Concern Regarding SPACs

Over the past year, FINRA's review of firms participating in SPAC offerings has focused on the following.

Due Diligence – When firms and associated persons act as underwriter, qualified independent underwriter or syndicate member for a SPAC offering, the due diligence conducted at the IPO and merger stages, including as to the relevant officers, directors and control persons of the SPAC and SPAC-sponsor(s) and pre-identified acquisition targets.

Reg BI – Written policies and procedures or guidance on recommendations to retail customers, and supervisory systems designed to identify and address conflicts of interest presented by the involvement of the firm, their associated persons or both.

Disclosure – Firms' supervision of associated persons who hold positions with, advise or personally invest in SPACs or SPAC sponsors, and whether the associated persons are disclosing their involvement if required by FINRA rules governing OBAs, PSTs and Form U4 amendments.

Net Capital – In firm-commitment underwritings, whether firms are correctly taking net capital charges relative to the size of their commitment or using a written agreement with another syndicate member (*i.e.,* "backstop provider").

WSPs and Supervisory Controls – whether firms are maintaining and regularly updating their WSPs and supervisory controls to address risks related to SPACs (*e.g.,* Reg BI, due diligence, information barrier policies, conflicts of interest).

In October 2021, FINRA initiated a targeted review to explore the above areas and other issues relating to SPACs. Additional review areas include training; the use of qualified independent underwriters; underwriting compensation; services provided to SPACs, their sponsors or affiliated entities; and potential merger targets. It is anticipated that, at a future date, FINRA will share with member firms its findings from this review.

Communications with the Public

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA Rule 2210 (Communications with the Public) defines all communications into three categories—correspondence, retail communications or institutional communications—and sets principles-based content standards that are designed to apply to ongoing developments in communications technology and practices. **New member firms are required to file retail communications with FINRA's Advertising Regulation Department during their first year of membership.** ★

FINRA Rule 2220 (Options Communications) governs members' communications with the public concerning options. Additionally, MSRB Rule G-21 (Advertising by Brokers, Dealers or Municipal Securities Dealers) contains similar content standards relating to municipal securities or concerning the facilities, services or skills of any municipal dealer.

Related Considerations:

- **General Standards –**
  - Do your firm's communications contain false, misleading or promissory statements or claims?
  - Do your firm's communications include material information necessary to make them fair, balanced and not misleading? For example, if a communication promotes the benefits of a high-risk or illiquid security, does it explain the associated risks?
  - Do your firm's communications balance specific claims of investment benefits from a securities product or service (especially complex products) with the key risks specific to that product or service?
  - Do your firm's communications contain predictions or projections of investment performance to investors that are generally prohibited by FINRA Rule 2210(d)(1)(F)?
- **Mobile Apps –**
  - **Has your firm established and implemented a comprehensive supervisory system for communications through mobile apps?**
  - **Have you tested the accuracy of account information, including labels and data, displayed in your mobile apps?**
  - **Do your mobile apps accurately describe how their features work?**
  - **Do your mobile apps identify information in ways that are readily understandable, based on the experience level of your customers?**
  - **Do your mobile apps provide investors with readily available information to explain complex strategies and investments and associated risks?**
  - **If your firm offers an app to retail customers, does the information provided to customers constitute a "recommendation" that would be covered by Reg BI, and in the case of recommendations of options or variable annuities, FINRA Rules 2360 (Options) or 2330 (Members' Responsibilities Regarding Deferred Variable Annuities)? If so, how does your firm comply with these obligations?**
- **Digital Communication Channels –**
  - Does your firm's digital communication policy address all permitted and prohibited digital communication channels and features available to your customers and associated persons?
  - Does your firm review for red flags that may indicate a registered representative is communicating through unapproved communication channels, and does your firm follow up on such red flags? For example, red flags might include email chains that copy unapproved representative email addresses, references in emails to communications that occurred outside approved firm channels or customer complaints mentioning such communications.
  - How does your firm supervise and maintain books and records in accordance with SEC and FINRA Books and Records Rules for all approved digital communications?
  - Does your firm have a process to confirm that all business-related communications comply with the content standards set forth in FINRA Rule 2210?
- **Digital Asset Communications** – If your firm or an affiliate engages in digital asset activities:
  - does your firm provide a fair and balanced presentation in marketing materials and retail communications, including addressing risks presented by digital asset investments and not misrepresenting the extent to which digital assets are regulated by FINRA or the federal securities laws or eligible for protections thereunder, such as Securities Investor Protection Corporation (SIPC) coverage?

- do your firm's communications misleadingly imply that digital asset services offered through an affiliated entity are offered through and under the supervision, clearance and custody of a registered broker-dealer?

- **Cash Management Accounts Communications** – If your firm offers Cash Management Accounts, does it:
  - clearly communicate the terms of the Cash Management Accounts?
  - disclose that the Cash Management Accounts' deposits are obligations of the destination bank and not cash balances held by your firm?
  - assure that its communications do not state or imply that:
    - brokerage accounts are similar to or the same as bank "checking and savings accounts" or other accounts insured by the Federal Deposit Insurance Corporation (FDIC); and
    - FDIC insurance coverage applies to funds when held at a registered broker-dealer?
  - review whether communications fairly explain the:
    - nature and structure of the program;
    - relationship of the brokerage accounts to any partner banks in the Cash Management Accounts;
    - amount of time it may take for customer funds to reach the bank accounts; and
    - benefits and risks of participating in such programs?
- **Municipal Securities Communications – If your firm offers municipal securities, does it confirm that advertisements for such securities include the necessary information to be fair, balanced and not misleading, and do not include:**
  - **exaggerated claims about safety or misleading comparisons to US Treasury Securities;**
  - **statements claiming "direct access" to bonds in the primary market if the firm is not an underwriter; and**
  - **unwarranted claims about the predictability or consistency of growth or payments?**
- **If an advertisement includes claims of municipal securities being "tax free," does it also explain any applicable state, local, alternative minimum tax, capital gains or other tax consequences?**
- **If an advertisement advertises a "taxable equivalent" yield on a municipal security offering, does it provide sufficient information regarding the tax bracket used to make the calculation?**

Exam Findings and Effective Practices

Exam Findings:

- **False, Misleading and Inaccurate Information in Mobile Apps –**
  - **Incorrect or misleading account balances or inaccurate information regarding accounts' historical performance.**
  - **Sending margin call warnings to customers whose account balances were not approaching, or were below, minimum maintenance requirements.**
  - **Falsely informing customers that their accounts were not enabled to trade on margin, when the accounts were, in fact, margin enabled.**
  - **Misstating the risk of loss associated with certain options transactions.**
  - **Distributing false and misleading promotions through social media and "push" notifications on mobile apps that made promissory claims or omitted material information.**

- **Deficient Communications Promoting Digital Assets –**
  - **Falsely identifying the broker-dealer as the entity from whom digital assets may be purchased or creating confusion about which entity is offering digital assets by using identical or substantially similar names to the broker dealer's name.**
- **Misrepresentations in Cash Management Account Communications –**
  - **Misleading statements or claims that either state or imply the broker-dealer is a bank.**
  - Misleading or false claims that state or imply the Cash Management Accounts are "checking and savings accounts."
  - Inaccurate or misleading statements concerning the amount of FDIC insurance coverage provided to investor funds when they are held at a partner bank.
  - Incomplete or inaccurate claims concerning the amount of time it may take for customer funds to reach the bank accounts or be available to investors once deposited at a partner bank.
  - Inaccurate or misleading claims about the actual terms of the Cash Management Accounts.
  - **Failure to balance promotional claims with the risks of participating in such programs.**
- **Insufficient Supervision and Recordkeeping for Digital Communications** – Not maintaining policies and procedures to reasonably identify and respond to red flags—such as customer complaints, representatives' email, OBA reviews or advertising reviews—that registered representatives used business-related digital communications methods not controlled by the firm, including texting, messaging, social media, collaboration apps or "electronic sales seminars" in chatrooms.
- **No WSPs and Controls for Communication That Use Non-Member or OBA Names (so-called "Doing Business As" or "DBA" Names) –**
  - Not maintaining WSPs to identify the broker-dealer clearly and prominently as the entity through which securities were offered in firm communications, such as websites, social media posts, seminars or emails that promote or discuss the broker-dealer's securities business and identify a non-member entity, such as a representative's OBA.
  - Not including a "readily apparent reference" and hyperlink to FINRA's BrokerCheck in such communications.
- **Municipal Securities Advertisements – Using false and misleading statements or claims about safety, unqualified or unwarranted claims regarding the expertise of the firm, and promissory statements and claims regarding portfolio growth.**

Effective Practices:

- **Comprehensive Procedures for Mobile Apps – Maintaining and implementing comprehensive procedures for the supervision of mobile apps, for example, that confirm:**
  - **data displayed to customers is accurate; and**
  - **information about mobile apps' tools and features complies with FINRA's communications and other relevant rules before it is posted to investors.**
- **Comprehensive Procedures for Digital Communications** – Maintaining and implementing procedures for supervision of digital communication channels, including:
  - **Monitoring of New Tools and Features** – Monitoring new communication channels, apps and features available to their associated persons and customers.

- **Defining and Enforcing What is Permissible and Prohibited** – Clearly defining permissible and prohibited digital communication channels and blocking prohibited channels, tools or features, including those that prevent firms from complying with their recordkeeping requirements.
- **Supervision** – Implementing supervisory review procedures tailored to each digital channel, tool and feature.
- **Video Content Protocols** – Developing WSPs and controls for live-streamed public appearances, scripted presentations or video blogs.
- **Training** – Implementing mandatory training programs prior to providing access to firm-approved digital channels, including expectations for business and personal digital communications and guidance for using all permitted features of each channel.
- **Disciplinary Action** – Temporarily suspending or permanently blocking from certain digital channels or features those registered representatives who did not comply with the policies and requiring them to take additional digital communications training.

- **Digital Asset Communications** – Maintaining and implementing procedures for firm digital asset communications, including:
  - **Risk Disclosure** – Prominently describing the risks associated with digital assets that are needed to balance any statements or claims contained in a digital asset communication, including that such investments are speculative, involve a high degree of risk, are generally illiquid, may have no value, have limited regulatory certainty, are subject to potential market manipulation risks and may expose investors to loss of principal.
  - **Communication Review** – Reviewing firms' communications to confirm that they were not exaggerating the potential benefits of digital assets or overstating the current or future status of digital asset projects or **platforms.**
  - **Communication to Differentiate Digital Assets From Broker-Dealer Products** – Identifying, segregating and differentiating firms' broker-dealer products and services from those offered by affiliates or third parties, including digital asset affiliates; and clearly and prominently identifying entities responsible for non-securities digital assets businesses (and explaining that such services were not offered by the broker-dealer or subject to the same regulatory protections as those available for securities).
- **Reviews of Firms' Capabilities for Cash Management Accounts** – Requiring new product groups or departments to conduct an additional review for proposed Cash Management Accounts to confirm that the firms' existing business processes, supervisory systems and compliance programs—especially those relating to communications—can support such programs.
- **Use of Non-Member or OBA Names (so-called DBAs)** – Maintaining and implementing procedures for OBA names, including:
  - **Prior Approval** – Prohibiting the use of OBA communications that concern the broker-dealer's securities business without prior approval by compliance and creating a centralized system for the review and approval of such communications, including content and disclosures.
  - **Training** – Providing training on relevant FINRA rules and firm policies and requiring annual attestations to demonstrate compliance with such requirements.
  - **Templates** – Requiring use of firm-approved vendors to create content or standardized templates populated with approved content and disclosures for all OBA communications (including websites, social media, digital content or other communications) that also concern the broker-dealer's securities business.
  - **Notification and Monitoring** – Requiring registered representatives to notify compliance of any changes to approved communications and conducting periodic, at least annual, monitoring and review of previously approved communications for changes and updates.

- **Municipal Securities Advertisements – Maintaining and implementing procedures for firm municipal securities communications, including:**
  - **Prior Approval – Requiring prior approval of all advertisements concerning municipal securities by an appropriately qualified principal to confirm the content complies with applicable content standards.**
  - **Training – Providing education and training for firm personnel on applicable FINRA and MSRB rules and firm policies.**
  - **Risk Disclosure – Balancing statements concerning the benefits of municipal securities by prominently describing the risks associated with municipal securities, including credit risk, market risk and interest rate risk.**
  - **Review – Reviewing firms' communications to confirm that the potential benefits of tax features are accurate and not exaggerated.**

Additional Resources

- *Regulatory Notice* 21-25 (FINRA Continues to Encourage Firms to Notify FINRA if They Engage in Activities Related to Digital Assets)
- *Regulatory Notice* 20-21 (FINRA Provides Guidance on Retail Communications Concerning Private Placement Offerings)
- *Regulatory Notice* 19-31 (Disclosure Innovations in Advertising and Other Communications with the Public)
- *Regulatory Notice* 17-18 (Guidance on Social Networking Websites and Business Communications)
- *Regulatory Notice* 11-39 (Social Media Websites and the Use of Personal Devices for Business Communications)
- *Regulatory Notice* 10-06 (Guidance on Blogs and Social Networking Web Sites)
- Advertising Regulation Topic Page
- FINRA's Social Media Topic Page
- ***MSRB Notice 2019-07***
- ***MSRB Notice 2018-18***

Private Placements

Regulatory Obligations and Related Considerations

Regulatory Obligations:

In *Regulatory Notice* 10-22 (Obligations of Broker-Dealers to Conduct Reasonable Investigations in Regulation D Offerings), FINRA noted that members that recommend private offerings have obligations under FINRA Rule 2111 (Suitability) and FINRA Rule 3110 (Supervision) to conduct reasonable diligence by evaluating "the issuer and its management; the business prospects of the issuer; the assets held by or to be acquired by the issuer; the claims being made; and the intended use of proceeds of the offering." **Although FINRA's Suitability Rule continues to apply to recommendations to non-retail customers, it no longer applies to recommendations to retail customers. Instead, the SEC's Reg BI applies to recommendations to retail customers of any securities transaction or investment strategy involving securities, including recommendations of private offerings.**

Additionally, firms must make timely filings for specified private placement offerings with FINRA's Corporate Financing Department under FINRA Rules 5122 (Private Placements of Securities Issued by Members) and 5123 (Private Placements of Securities), and should also be aware of recent amendments to these rules.[12] ★

Related Considerations:

- What policies and procedures does your firm have to address filing requirements and timelines under FINRA Rules 5122 and 5123? How does it review for compliance with such policies?
- How does your firm confirm that associated persons conduct reasonable diligence prior to recommending private placement offerings, including conducting further inquiry into red flags?
- How does your firm address red flags regarding conflicts of interest identified during the reasonable diligence process and in third-party due diligence reports?
- How does your firm manage the transmission of funds and amended terms in contingency offerings, including ensuring compliance with Securities Exchange Act Rules 10b-9 and 15c2-4, as applicable?

Exam Findings and Effective Practices

Exam Findings:

- **Late Filings** – Not having policies and procedures, processes and supervisory programs to comply with filing requirements; and failing to make timely filings (with, in some cases, delays lasting as long as six to 12 months after the offering closing date).
- **No Reasonable Diligence** – Failing to perform reasonable diligence of private placement offerings prior to recommending them to retail investors, including:
  - **failing to conduct an appropriate level of research, particularly when the firm lacks experience or specialized knowledge pertaining to an issuer's underlying business or when an issuer lacks an operating history;**
  - **relying unreasonably on the firm's experience with the same issuer in previous offerings;** and
  - failing to inquire into and analyze red flags identified during the reasonable-diligence process or in third-party due diligence reports.

Effective Practices:

- **Private Placement Checklist** – Creating checklists with—or adding to existing due diligence checklists—all steps, filing dates and related documentation requirements, noting staff responsible for performing functions and tasks and evidence of supervisory principal approval for the reasonable diligence process and the filing requirements of FINRA Rules 5122 and 5123.
- **Independent Research** – Conducting and documenting independent research on material aspects of the offering; identifying any red flags with the offering or the issuer (such as questionable business plans or unlikely projections or results); and addressing and, if possible, resolving concerns that would be deemed material to a potential investor (such as liquidity restrictions).
- **Independent Verification** – Verifying information that is key to the performance of the offering (such as unrealistic costs projected to execute the business plan, coupled with aggressively projected timing and overall rate of return for investors), in some cases with support from law firms, experts and other third-party vendors.

- **Identifying Conflicts of Interest** – Using firms' reasonable diligence processes to identify conflicts of interest (*e.g.,* firm affiliates or issuers whose control persons were also employed by the firm) and then addressing such conflicts (such as by confirming that the issuer prominently and comprehensively discloses these conflicts in offering documents or mitigating them by removing financial incentives to recommend a private offering over other more appropriate investments).
- **Responsibility for Reasonable Diligence and Compliance** – Assigning responsibility for private placement reasonable diligence and compliance with filing requirements to specific individual(s) or team(s) and conducting targeted, in-depth training about the firms' policies, process and filing requirements.
- **Alert System** – Creating a system that alerts responsible individual(s) and supervisory principal(s) about upcoming and missed filing deadlines.
- **Post-Closing Assessment** – Conducting reviews after the offering closes to ascertain whether offering proceeds were used in a manner consistent with the offering memorandum.

Additional Resources

- ***Regulatory Notice* 21-26 (FINRA Amends Rules 5122 and 5123 Filing Requirements to Include Retail Communications That Promote or Recommend Private Placements)**
- ***Regulatory Notice* 21-10 (FINRA Updates Private Placement Filer Form Pursuant to FINRA Rules 5122 and 5123)**
- ***Regulatory Notice* 20-21 (FINRA Provides Guidance on Retail Communications Concerning Private Placement Offerings)**
- *Regulatory Notice* 10-22 (Obligations of Broker-Dealers to Conduct Reasonable Investigations in Regulation D Offerings)
- Report Center – Corporate Financing Report Cards
- FAQs about Private Placements
- Corporate Financing Private Placement Filing System User Guide
- Private Placements Topic Page

Conservation Donation Transactions Risks

FINRA is seeing continued syndications of Conservation Donation Transactions (CDTs) investment programs among broker-dealers. CDTs commonly involve private placement offerings where investor returns are based on a share of tax savings from a charitable donation. In practice, CDTs involve unrelated investors acquiring an interest in a passthrough entity (*i.e.,* a partnership or limited liability company) owning unimproved land. Before year-end, the passthrough entity either grants a conservation easement—which forever limits future development of the land—or outright donates the land to a land trust. In exchange, the passthrough entity receives charitable donation tax deductions, which serve as a return on investment to investors and often have values based solely on land appraisals that are predicated on an alternative plan to develop the land, oftentimes the equivalent of four to more than 10 times the price paid to acquire the land. (Common CDTs involve syndicated conservation easement transactions (SCETs) or substantially similar, fee simple donations of land.)

Firms that engage in CDTs should consider the following questions to determine whether they meet regulatory obligations:

- Do the CDT sponsor, appraiser or other related service providers have any prior, adverse audit history?
- Do your firm's offering disclosures present potential conflicts of interest among sponsors, consultants, land developers, prior landowners, broker-dealers, and registered persons having employment or affiliated relationships?
- In compliance with Reg BI, does your firm:
  - consider reasonably available alternatives to any recommendation of CDTs (*i.e.,* the Care Obligation);
  - have policies and procedures to identify and—at a minimum—disclose or eliminate all conflicts of interest associated with the recommendation (*i.e.,* the Conflicts of Interest Obligation); and
  - have policies and procedures to identify and mitigate any conflicts of interest associated with recommendations of CDTs that create an incentive for an associated person to place the interest of the firm or the associated person ahead of the retail customer's interest?
- In compliance with SEA Rule 15c2-4, does your firm promptly transmit funds to either an escrow agent or a separate bank account (as CDTs are typically associated with contingent offerings)?
- How does your firm establish and document reasonable diligence of CDTs, including further inquiries in the presence of red flags (*e.g.,* CDTs resulting in donation deductions that are more than two-and-one-half times an investor's investment, concerns surfaced in third-party due diligence reports, large markups associated with land acquisition, certain types of fees to related parties, marketing communications promoting CDTs solely on their tax benefits)?

For additional guidance, please refer to these resources:

- FINRA, 2018 Report on Examination Findings – Reasonable Diligence for Private Placements (Dec. 7, 2018)
- United States Senate, Report on Syndicated Conservation-Easement Transactions
- Internal Revenue Service, IRS increases enforcement action on Syndicated Conservation Easements (Nov. 12, 2019)
- Internal Revenue Service, IRS concludes "Dirty Dozen" list of tax scams for 2019: Agency encourages taxpayers to remain vigilant year-round (Mar. 20, 2019)
- Land Trust Alliance, Important Advisory: Tax Shelter Abuse of Conservation Donations (Feb. 1, 2018)
- Internal Revenue Service, Notice 2017-10, Listing Notice – Syndicated Conservation Easement Transactions

Variable Annuities

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA Rule 2330 (Members' Responsibilities Regarding Deferred Variable Annuities) establishes sales practice standards regarding recommended purchases and exchanges of deferred variable annuities. To the extent that a broker-dealer or associated person is recommending a purchase or exchange of a deferred variable annuity to a retail customer, Reg BI's obligations, discussed above, also would apply.

In addition, Rule 2330 requires firms to establish and maintain specific written supervisory procedures reasonably designed to achieve compliance with the rule. Firms must implement surveillance procedures to determine if any associated person is effecting deferred variable annuity exchanges at a rate that might suggest conduct inconsistent with FINRA Rule 2330 and any other applicable FINRA rules or the federal securities laws.

Related Considerations:

- How does your firm review for rates of variable annuity exchanges (*i.e.,* does your firm use any automated tools, exception reports or surveillance reports)?
- Does your firm have standardized review thresholds for rates of variable annuity exchanges?
- Does your firm have a process to confirm its variable annuity data integrity (including general product information, share class, riders and exchange-based activity) and engage with affiliate and non-affiliate insurance carriers to address inconsistencies in available data, data formats and reporting processes for variable annuities?
- How do your firm's WSPs support a determination that a variable annuity exchange has a reasonable basis? How do you obtain, evaluate and record relevant information, such as:
  - loss of existing benefits;
  - increased fees or charges;
  - surrender charges, or the establishment or creation of a new surrender period;
  - consistency of customer liquid net worth invested in the variable annuity with their liquidity needs;
  - whether a share class is in the customer's best interest, given his or her financial needs, time horizon and riders included with the contract; and
  - prior exchanges within the preceding 36 months?
- Do your firm's policies and procedures require registered representatives to inform customers of the various features of recommended variable annuities such as surrender charges, potential tax penalties, various fees and costs, and market risk?
- What is the role of your registered principals in supervising variable annuity transactions, including verifying how the customer would benefit from certain features of deferred variable annuities (*e.g.,* tax-deferral, annuitization, or a death or living benefit)? What processes, forms, documents and information do the firm's registered principals rely on to make such determinations?
- **What is your firm's process to supervise registered representatives who advise their clients' decisions whether or not to accept a buyout offer?**

Exam Findings and Effective Practices

Exam Findings:

- **Exchanges** – Not reasonably supervising recommendations of exchanges for compliance with FINRA Rule 2330 and Reg BI, leading to exchanges that were inconsistent with the customer's objectives and time horizon and resulted in, among other consequences, increased fees to the customer or the loss of material, paid-for accrued benefits.
- **Insufficient Training** – Not conducting training for registered representatives and supervisors regarding how to assess costs and fees, surrender charges and long-term income riders to determine whether exchanges were suitable for customers.
- **Poor and Insufficient Data Quality – Not collecting and retaining key information on variable annuity transactions, particularly in connection with exchange transactions; relying on processes for data collection and retention in situations where the volume of variable annuity transactions renders these processes ineffective; and failing to address inconsistencies in available data for variable annuities, as well as data formats and reporting processes.**
- **Issuer Buyouts** – Not reasonably supervising recommendations related to issuer buyout offers (*e.g.,* associated persons' recommendations that investors surrender the contract in order to generate an exchange or new purchase) for compliance with FINRA Rule 2230 and Reg BI.

Effective Practices:

- **Automated Surveillance** – Using automated tools, exception reports and surveillance to review variable annuity exchanges; and implementing second-level supervision of supervisory reviews of exchange-related exception reports and account applications.
- **Rationales** – Requiring registered representatives to provide detailed written rationales for variable annuity exchanges for each customer (including confirming that such rationales address the specific circumstances for each customer and do not replicate rationales provided for other customers); and requiring supervisory principals to verify the information provided by registered representatives, including product fees, costs, rider benefits and existing product values.
- **Review Thresholds** – Standardizing review thresholds for rates of variable annuity exchanges; and monitoring for emerging trends across registered representatives, customers, products and branches.
- **Automated Data Supervision – Creating automated solutions to synthesize variable annuity data (including general product information, share class, riders and exchange-based activity) in situations warranted by the volume of variable annuity transactions.**
- **Data Integrity** – Engaging with insurance carriers (affiliated and non-affiliated) and third-party data providers (*e.g.,* DTCC and consolidated account report providers) to address inconsistencies in available data, data formats and reporting processes for variable annuities.
- **Data Acquisition – Establishing a supervisory system that collects and utilizes key transaction data, including, but not limited to:**
  - **transaction date;**
  - **rep name;**
  - **customer name;**
  - **customer age;**
  - **investment amount;**
  - **whether the transaction is a new contract or an additional investment;**
  - **contract type (qualified vs. non-qualified);**

- **contract number;**
- **product issuer;**
- **product name;**
- **source of funds;**
- **exchange identifier;**
- **share class; and**
- **commissions.**

- **Data Analysis – Considering the following data points when conducting a review of an exchange transaction under FINRA Rule 2330 and Reg BI:**
  - **branch location;**
  - **customer state of residence;**
  - **policy riders;**
  - **policy fees;**
  - **issuer of exchanged policy;**
  - **exchanged policy product name;**
  - **date exchanged policy was purchased;**
  - **living benefit value, death benefit value or both, that was forfeited;**
  - **surrender charges incurred; and**
  - **any additional benefits surrendered with forfeiture.**

Additional Resources

- SEC
  - Regulation Best Interest, Form CRS and Related Interpretations
- FINRA
  - Regulation Best Interest (Reg BI) Topic Page
  - *Regulatory Notice* 20-18 (FINRA Amends Its Suitability, Non-Cash Compensation and Capital Acquisition Broker (CAB) Rules in Response to Regulation Best Interest)
  - *Regulatory Notice* 20-17 (FINRA Revises Rule 4530 Problem Codes for Reporting Customer Complaints and for Filing Documents Online)
  - *Regulatory Notice* 10-05 (FINRA Reminds Firms of Their Responsibilities Under FINRA Rule 2330 for Recommended Purchases or Exchanges of Deferred Variable Annuities)
  - *Notice to Members* 07-06 (Special Considerations When Supervising Recommendations of Newly Associated Registered Representatives to Replace Mutual Funds and Variable Products)
  - *Notice to Members* 99-35 (The NASD Reminds Members of Their Responsibilities Regarding the Sales of Variable Annuities)
  - Variable Annuities Topic Page

Market Integrity

Consolidated Audit Trail (CAT)

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA and the national securities exchanges have adopted rules requiring their members to comply with Exchange Act Rule 613 and the CAT NMS Plan FINRA Rule 6800 Series (Consolidated Audit Trail Compliance Rule) (collectively, CAT Rules), which cover reporting to the CAT; clock synchronization; time stamps; connectivity and data transmission; development and testing; recordkeeping; and timeliness, accuracy and completeness of data requirements. *Regulatory Notice* 20-31 (FINRA Reminds Firms of Their Supervisory Responsibilities Relating to CAT) describes practices and recommended steps firms should consider when developing and implementing their CAT Rules compliance program.

Related Considerations:

- Do your firm's CAT Rules WSPs: (1) identify the individual, by name or title, responsible for the review of CAT reporting; (2) describe specifically what type of review(s) will be conducted of the data posted on the CAT Reporter Portal; (3) specify how often the review(s) will be conducted; and (4) describe how the review(s) will be evidenced?
- How does your firm confirm that the data your firm reports, or that is reported on your firm's behalf, is transmitted in a timely fashion and is complete and accurate?
- How does your firm determine how and when clocks are synchronized, who is responsible for clock synchronization, how your firm evidences that clocks have been synchronized and how your firm will self-report clock synchronization violations?
- Does your firm conduct daily reviews of the Industry Member CAT Reporter Portal (CAT Reporter Portal) to review file status to confirm the file(s) sent by the member or by their reporting agent was accepted by CAT and to identify and address any file submission or integrity errors?
- Does your firm conduct periodic comparative reviews of accepted CAT data against order and trade records and the CAT Reporting Technical Specifications?
- Does your firm communicate regularly with your CAT reporting agent, review relevant CAT guidance and announcements and report CAT reporting issues to the FINRA CAT Help Desk?
- **Does your firm maintain the required CAT order information as part of its books and records and in compliance with FINRA Rule 6890 (Recordkeeping)?**
- **How does your firm work with its clearing firm and third-party vendors to maintain CAT compliance?**

Exam Findings and Effective Practices

Exam Findings:

- **Inaccurate Reporting of CAT Orders – Submitting information that was incorrect, incomplete or both to the Central Repository, such as:**
  - **account holder type;**
  - **buy/sell side;**
  - **cancel quantity;**
  - **route event quantity (*e.g.,* reporting an old quantity that had been modified to a different amount);**

- **trading session code;**
- **new order code;**
- **department type code (*e.g.,* reporting "A" for agent, when the firm does not execute orders);**
- **time in force;**
- **handling instructions (*e.g.,* reporting new order events as Stop on Quote (SOQ) or Stop Limit on Quote (SLQ)); and**
- **representative indicator (*i.e.,* reporting the representative indicator to reflect a representative order when the order in a firm account was not created for the purpose of working one or more customer or client orders).**

- **Late Resolution of Repairable CAT Errors – Not resolving repairable CAT errors in a timely manner (*i.e.,* within the T+3 requirement).**
- **Inadequate Vendor Supervision – Not establishing and maintaining WSPs or supervisory controls regarding both CAT reporting and clock synchronization that are performed by third-party vendors.**

Effective Practices:

- **Supervision – Implementing a comparative review of CAT submissions versus firm order records; and utilizing CAT Report Cards and CAT FAQs to design an effective supervision process.**
- **Clock Synchronization Related to Third Parties – Obtaining adequate information from third parties to meet applicable clock synchronization requirements.[13]**

Additional Resources

- CAT NMS Plan
- FINRA
  - Consolidated Audit Trail (CAT) Topic Page
  - Equity Report Cards
  - *Regulatory Notice* 20-31 (FINRA Reminds Firms of Their Supervisory Responsibilities Relating to CAT)
  - *Regulatory Notice* 19-19 (FINRA Reminds Firms to Register for CAT Reporting by June 27, 2019)
  - *Regulatory Notice* 17-09 (The National Securities Exchanges and FINRA Issue Joint Guidance on Clock Synchronization and Certification Requirements Under the CAT NMS Plan)

Best Execution

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA Rule 5310 (Best Execution and Interpositioning) requires that, in any transaction for or with a customer or a customer of another broker-dealer, a member firm and persons associated with a member firm 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. Where a firm may choose to not conduct an order-by-order review—to the extent consistent with Rule 5310 and associated guidance—it must have procedures in place to confirm it periodically conducts "regular and rigorous" reviews of the execution quality of its customers' orders.

Best execution obligations apply to any member firm that receives customer orders—for purposes of handling and execution—including firms that receive orders directly from customers, as well as those that receive customer orders from other firms for handling and execution, such as wholesale market makers.[14] These obligations also apply when a firm acts as agent for the account of its customer and executes transactions as principal. Any firm subject to FINRA Rule 5310 cannot transfer its duty of best execution to another person; additionally, any firm that routes all of its customer orders to another firm without conducting an independent review of execution quality would violate its duty of best execution.

Related Considerations:

- How does your firm determine whether to employ order-by-order or "regular and rigorous" reviews of execution quality?
- If applicable, how does your firm implement and conduct an adequate "regular and rigorous" review of the quality of the executions of its customers' orders and orders from a customer of another broker-dealer?
- If applicable, how does your firm document its "regular and rigorous" reviews, the data and other information considered, order routing decisions and the rationale used, and address any deficiencies?
- **How does your firm compare the execution quality received under its existing order routing and execution arrangements (including the internalization of order flow) to the quality of the executions it could obtain from competing markets (whether or not the firm already has routing arrangements with them), including off-exchange trading venues?**
- **How does your firm address potential conflicts of interest in order routing decisions, including those involving:**
  - **affiliated entities (*e.g.,* affiliated broker-dealers, affiliated alternative trading systems (ATSs));**
  - **market centers, including off-exchange trading venues, that provide payment for order flow (PFOF) or other order-routing inducements; and**
  - **orders from customers of another broker-dealer for which your firm provides PFOF?**
- **If your firm provides PFOF to another broker-dealer, how does your firm prevent those payments from interfering with your firm's best execution obligations (including situations where you provide PFOF and execute the covered orders)?**
- If your firm engages in fixed income and options trading, has it established targeted policies and procedures to address its best execution obligations for these products?
- Does your firm consider differences among security types within these products, such as the different characteristics and liquidity of U.S. Treasury securities compared to other fixed income securities?
- How does your firm meet its best execution obligations with respect to trading conducted in both regular and extended trading hours?
- Does your firm consider the risk of information leakage affecting pricing when assessing the execution quality of orders routed to a particular venue?
- What data sources does your firm use for its routing decisions and execution quality reviews for different order types and sizes, including odd lots?
- How does your firm handle fractional share investing in the context of its best execution obligations?

Exam Findings and Effective Practices

Exam Findings:

- **No Assessment of Execution in Competing Markets** – Not comparing the quality of the execution obtained via firms' existing order-routing and execution arrangements against the quality of execution they could have obtained from competing markets.

- **No Review of Certain Order Types** – Not conducting adequate reviews on a type-of-order basis, including, for example, on market, marketable limit, or non-marketable limit orders.
- **No Evaluation of Required Factors** – Not considering certain factors set forth in Rule 5310 when conducting a "regular and rigorous review," including, among other things, speed of execution, price improvement and the likelihood of execution of limit orders; and using routing logic that was not necessarily based on quality of execution.
- **Conflicts of Interest** – Not considering and addressing potential conflicts of interest relating to routing orders to affiliated broker-dealers, affiliated ATSs, or market centers that provide routing inducements, such as PFOF from wholesale market makers and exchange liquidity rebates.

Targeted Reviews of Wholesale Market Makers

FINRA is conducting targeted best execution reviews of wholesale market makers concerning their relationships with broker-dealers that route orders to them as well as their own order routing practices and decisions (with respect to these orders). These targeted reviews are evaluating:

- whether wholesale market makers are conducting adequate execution quality reviews;
- whether order routing, handling and execution arrangements (including PFOF agreements) with retail broker-dealers have an impact on the wholesale marker makers' order handling practices and decisions, and fulfillment of their best execution obligations; and
- any modified order handling procedures that the wholesale market makers implemented during volatile or extreme market conditions.

Effective Practices:

- **Exception Reports** – Using exception reports and surveillance reports to support firms' efforts to meet their best execution obligations.
- **PFOF Order Handling Impact Review** – Reviewing how PFOF affects the order-handling process, including the following factors: any explicit or implicit contractual arrangement to send order flow to a third-party broker-dealer; terms of these agreements; whether it is on a per-share basis or per-order basis; and whether it is based upon the type of order, size of order, type of customer or the market class of the security.
- **Risk-Based "Regular and Rigorous Reviews"** – Conducting "regular and rigorous" reviews, at a minimum, on a quarterly or more frequent basis (such as monthly), depending on the firm's business model.
- **Continuous Updates** – Updating WSPs and best execution analysis to address market and technology changes.

Additional Resources

- ***Regulatory Notice* 21-23 (FINRA Reminds Member Firms of Requirements Concerning Best Execution and Payment for Order Flow)**
- ***Regulatory Notice* 21-12 (FINRA Reminds Member Firms of Their Obligations Regarding Customer Order Handling, Margin Requirements and Effective Liquidity Management Practices During Extreme Market Conditions)**
- *Regulatory Notice* 15-46 (Guidance on Best Execution Obligations in Equity, Options and Fixed Income Markets)
- *Notice to Members* 01-22 (NASD Regulation Reiterates Member Firm Best Execution Obligations And Provides Guidance to Members Concerning Compliance)
- FINRA Report Center
- Equity Report Cards
- Best Execution Outside-of-the-Inside Report Card

Disclosure of Routing Information NEW FOR 2022

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Rule 606 of Regulation NMS requires broker-dealers to disclose information regarding the handling of their customers' orders in NMS stocks and listed options. These disclosures are designed to help customers: better understand how their firm routes and handles their orders; assess the quality of order handling services provided by their firm; and ascertain whether the firm is effectively managing potential conflicts of interest that may impact their firm's routing decisions.

Related Considerations:

- Does the firm publish accurate, properly formatted quarterly routing reports on its website for the required retention period as specified under Rule 606(a), including use of the SEC's most recently published PDF and XML schema?
- If the firm is not required to publish a quarterly report under Rule 606(a), does the firm have an effective supervisory process to periodically confirm that the firm has no orders subject to quarterly reporting?
- If the firm routes orders to non-exchange venues, does the firm adequately assess whether such venues are covered under Rule 606(a)?
- If the firm routes orders to non-exchange venues, does the firm obtain and retain sufficient information from such venues to properly report the material terms of its relationships with such venues, including specific quantitative and qualitative information regarding PFOF and any profit-sharing relationship?
- If the firm claims an exemption from providing not held order reports under Rule 606(b)(3) pursuant to Rule 606(b)(4) or (5), what policies and procedures does the firm have in place to determine if the firm's or a customer's order activity falls below the relevant *de minimis* thresholds?
- If the firm is required to provide customer-specific disclosures under Rule 606(b)(3), does the firm provide accurate, properly formatted disclosures for the prior six months to requesting customers within seven business days of receiving the request?

Exam Findings and Effective Practices

Exam Findings:

- **Inaccurate Quarterly Reports** – Publishing inaccurate information in the quarterly report on order routing, such as:
  - reporting only held orders in listed options, instead of both held and not held orders;
  - incorrectly stating that the firm does not have a profit-sharing arrangement or receive PFOF from execution venues;
  - not including payments, credits or rebates (whether received directly from an exchange or through a pass-through arrangement) in the "Net Payment Paid/Received" and "Material Aspects" sections of the quarterly report;
  - not including exchange pricing arrangements (*e.g.,* tiered pricing) in the "Net Payment Paid/Received" and "Material Aspects" sections of the quarterly report;
  - not disclosing any amounts of "Net Payment Paid/Received", when the firm receives PFOF for at least one of the four order types (*i.e.,* Market Orders, Marketable Limit Orders, Non-Marketable Limit Orders, Other Orders);
  - inaccurately identifying reported execution venues as "Unknown";
  - inaccurately identifying firms as execution venues (*e.g.,* identifying routing broker-dealer as execution venue, rather than the exchange where transactions are actually executed);

- incorrectly listing an entity as an execution venue when that entity does not execute trades (*e.g.,* firm that re-routes, but does not execute, orders; options consolidator that does not provide liquidity); and
- not posting the quarterly report on their firm's website in both required formats (*i.e.,* PDF and XML schema).

- **Incomplete Disclosures** – Not adequately describing material aspects of their relationships with disclosed venues in the Material Aspects disclosures portion of the quarterly report, such as:
  - inadequate descriptions of specific terms of PFOF and other arrangements (*e.g.,* "average" amounts of PFOF rather than specific disclosure noting the payment types, specific amount received for each type of payment, terms and conditions of each type of payment);
  - ambiguous descriptions of receipt of PFOF (*e.g.,* firm "may" receive payment);
  - inadequate or incomplete descriptions of PFOF received through pass-through arrangements;
  - incomplete descriptions of exchange credits or rebates; and
  - incomplete descriptions of tiered pricing arrangements, including the specific pricing received by the firm.
- **Deficient Communications** – Not notifying customers in writing of the availability of information specified under Rule 606(b)(1), as required by Rule 606(b)(2).[15]
- **Insufficient WSPs** – Either not establishing or not maintaining adequate WSPs reasonably designed to achieve compliance with the new requirements of Rule 606, including:
  - not updating their Disclosure of Order Routing Information WSPs to include new requirements detailed in amended Rule 606(a)(1) or new Rule 606(b)(3);
  - not describing the steps taken to review whether firms verified the data integrity of information sent to, or received from, their vendor—or not stating how the review would be evidenced by the reviewer;
  - not articulating a supervisory method of review to verify the accuracy, format, completeness, timely processing and details of the new Rule 606(b)(3) report, if requested, as well as documenting the performance of that review; and
  - not requiring the inclusion of detailed information regarding the routing and execution of the firm's customers' listed options orders in quarterly reports or customer-requested order routing disclosures.

Effective Practices:

- **Supervision** – Conducting regular, periodic supervisory reviews of the public quarterly reports and customer-specific order disclosure reports, if applicable, for accuracy (*e.g.,* assuring that per-venue disclosures of net aggregate PFOF and other payments are accurately calculated) and completeness (*e.g.,* assuring that the Material Aspects section adequately describes the firm's PFOF and other payment arrangement for each execution venue, including all material aspects that may influence the firm's order routing decisions).
- **Due Diligence on Vendors** – Performing due diligence to assess the accuracy of public quarterly reports and customer-specific order disclosure reports provided by third-party vendors by, for example, holding periodic meetings with vendors to review content of reports, comparing order samples against vendor-provided information, and confirming with the vendor that all appropriate order information is being received (particularly when the firm has complex routing arrangements with execution venues).

Additional Resources

- SEC's 2018 Amendments to Rule 606 of Regulation NMS
- SEC's Responses to Frequently Asked Questions Concerning Rule 606 of Regulation NMS
- SEC's Staff Legal Bulletin No. 13A: Frequently Asked Questions About Rule 11Ac1-6
- SEC's Order Routing and Handling Data Technical Specification

Market Access Rule

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Exchange Act Rule 15c3-5 (Market Access Rule) requires firms 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." **The Market Access Rule applies generally to securities traded on an exchange or alternative trading system, including equities, equity options, exchange-traded funds (ETFs), debt securities, security-based swaps, security futures products, as well as digital assets that meet the SEC's definition of a security.**

Related Considerations:

- If your firm has or provides market access, does it have reasonably designed risk-management controls and WSPs to manage the financial, regulatory or other risks associated with this business activity?
- If your firm is highly automated, how does it manage and deploy technology changes for systems associated with market access and what controls does it use, such as kill switches, to monitor and respond to aberrant behavior by trading algorithms or other impactful market-wide events?
- How does your firm adjust credit limit thresholds for customers, including institutional customers (whether temporary or permanent)?
- Does your firm use any automated controls to timely revert ad hoc credit limit adjustments?
- If your firm uses third-party vendor tools to comply with its Market Access Rule obligations, does it review whether the vendor can meet the obligations of the rule?
- How does your firm maintain direct and exclusive control of applicable thresholds?
- What type of training does your firm provide to individual traders regarding the steps and requirements for requesting ad hoc credit limit adjustments?
- Does your firm test its market access controls, including fixed income controls, and how do you use that test for your firm's annual CEO certification attesting to your firm's controls?
- **If your firm operates an ATS that has subscribers that are not broker-dealers, how does your firm comply with the requirements of the Market Access Rule, including establishing, documenting and maintaining a system of controls and supervisory procedures reasonably designed to manage the financial, regulatory and other risks of this business activity?**

Exam Findings and Effective Practices

Exam Findings:

- **Insufficient Controls** – No pre-trade order limits, pre-set capital thresholds and duplicative and erroneous order controls for accessing ATSs, including those that transact fixed income transactions; not demonstrating the reasonability of assigned capital and credit pre-trade financial control thresholds; inadequate policies and procedures to govern intra-day changes to firms' credit and capital thresholds, including requiring or obtaining approval prior to adjusting credit or capital thresholds, documenting justifications for any adjustments and ensuring thresholds for temporary adjustments revert back to their pre-adjusted values.
- **Inadequate Financial Risk Management Controls** – For firms with market access, or those that provide it, unreasonable capital thresholds for trading desks, and unreasonable aggregate daily limits or credit limits for institutional customers and counterparties.
- **Reliance on Vendors** – Relying on third-party vendors' tools, including those of an ATS or exchange, to apply their financial controls without performing adequate due diligence, not understanding how vendors' controls

operate, or both; and not maintaining direct and exclusive control over controls by allowing the ATS to unilaterally set financial thresholds for firms' fixed income orders without the involvement of the firm, instead of establishing their own thresholds (some firms were not sure what their thresholds were and had no means to monitor their usage during the trading day).

Effective Practices:

- **Pre-Trade Fixed Income Financial Controls** – Implementing systemic pre-trade "hard" blocks to prevent fixed income orders from reaching an ATS that would cause the breach of a threshold.
- **Intra-Day *Ad Hoc* Adjustments** – Implementing processes for requesting, approving, reviewing and documenting ad hoc credit threshold increases and returning limits to their original values as needed.
- **Tailored Erroneous or Duplicative Order Controls** – Tailoring erroneous or duplicative order controls to particular products, situations or order types, and preventing the routing of market orders based on impact (Average Daily Volume Control) that are set at reasonable levels (particularly in thinly traded securities); and calibrating to reflect, among other things, the characteristics of the relevant securities, the business of the firm and market conditions.
- **Post-Trade Controls and Surveillance** – When providing direct market access via multiple systems, including sponsored access arrangements, employing reasonable controls to confirm that those systems' records were aggregated and integrated in a timely manner and conducting holistic post-trade and supervisory reviews for, among other things, potentially manipulative trading patterns.
- **Testing of Financial Controls** – Periodically testing their market access controls, which forms the basis for an annual CEO certification attesting to firms' controls.

Additional Resources

- *Regulatory Notice* 16-21 (SEC Approves Rule to Require Registration of Associated Persons Involved in the Design, Development or Significant Modification of Algorithmic Trading Strategies)
- *Regulatory Notice* 15-09 (Guidance on Effective Supervision and Control Practices for Firms Engaging in Algorithmic Trading Strategies)
- FINRA's Algorithmic Trading Topic Page
- FINRA's Market Access Topic Page
- **SEC's Responses to Frequently Asked Questions Concerning Risk Management Controls for Brokers or Dealers with Market Access**

Financial Management

Net Capital

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Exchange Act Rule 15c3-1 (Net Capital Rule) requires that firms must at all times have and maintain net capital at no less than the levels specified pursuant to the rule to protect customers and creditors from monetary losses that can occur when firms fail. Exchange Act Rule 17a-11 requires firms to notify FINRA in the event their net capital falls below the minimum amount required by the Net Capital Rule.

If firms have an affiliate paying any of their expenses, *Notice to Members* 03-63 (SEC Issues Guidance on the Recording of Expenses and Liabilities by Broker/Dealers) provides guidance for establishing an Expense Sharing Agreement that meets the standards set forth in Exchange Act Rule 17a-3[16]; firms with office leases should apply the guidance in *Regulatory Notice* 19-08 (Guidance on FOCUS Reporting for Operating Leases) for reporting lease assets and lease liabilities on their FOCUS reports. Additionally, firms must align its revenue recognition practices with the requirements of the Financial Accounting Standards Board's Topic 606 (Revenue from Contracts with Customers). ★

Related Considerations:

- How does your firm review its net capital treatment of assets to confirm that they are correctly classified for net capital purposes?
- How does your firm confirm that it has correctly identified and aged all failed to deliver contracts, properly calculated the applicable net capital charges and correctly applied the deductions to its net capital calculation?
- For firms with expense-sharing agreements, what kind of allocation methodology does your firm use and what kind of documentation does your firm maintain to substantiate its methodology for allocating specific broker-dealer costs to the firm or an affiliate?

Exam Findings and Effective Practices

Exam Findings:

- **Inaccurate Classification of Receivables, Liabilities and Revenue** – Incorrectly classifying receivables, liabilities and revenues, which resulted in inaccurate reporting of firms' financial positions and in some instances, a capital deficiency; incorrectly classifying non-allowable assets, such as large investments in certificates of deposit (CDs) because firms did not have a process to assess the net capital treatment of CDs pursuant to Exchange Act Rule 15c3-1(c)(2)(vi)(E); and not reviewing account agreements for CDs to determine whether they contained stipulations restricting withdrawals prior to maturity, including stipulations giving the bank discretion to permit or prohibit their withdrawal.
- **Failed to Deliver and Failed to Receive Contracts (Fails)** – Not having a process to correctly identify, track and age intra-month and end-of-the-month Fails for firms operating an Exchange Act Rule 15a-6 chaperoning business, including:
  - **Inaccurate Net Capital Charge** – Failing to compute and apply the correct applicable net capital charge for aged Fails;
  - **No Information from Clearing Firm** – Failing to request or confirm receipt of timely information relating to Fails from their clearing firms;
  - **Gaps in Policies and Procedures** – Failing to address monitoring, reporting and aging of Fails in firms' policies and procedures;
  - **Incorrect Balance Sheets and FOCUS Reports** – Failing to record Fails on firms' balance sheets, and as a result, filing incorrect FOCUS reports; and
  - **No Blotters** – Failing to maintain blotters for Fails.

- **Incorrect Capital Charges for Underwriting Commitments** – Not maintaining an adequate process to assess moment-to-moment and open contractual commitment capital charges on underwriting commitments, and not understanding their role as it pertained to the underwriting (*i.e.,* best efforts or firm commitment).
- **Inaccurate Recording of Revenue and Expenses** – Using cash accounting to record revenue and expenses as of the date the money changes hands, rather than accrual accounting (where firms would record revenue and expenses as of the date that revenue is earned or expenses are incurred); and making ledger entries as infrequently as once per month, as a result of which firms did not have adequate context to determine the proper accrual-based transaction date.
- **Insufficient Documentation Regarding Expense-Sharing Agreements** – Not delineating a method of allocation for payment; not allocating (fixed or variable) expenses proportionate to the benefit to the broker-dealer; or not maintaining sufficient documentation to substantiate firms' methodologies for allocating specific broker-dealer costs—such as technology fees, marketing charges, retirement account administrative fees and employees' compensation—to broker-dealers or affiliates.

Effective Practices:

- **Net Capital Assessment** – Performing an assessment of net capital treatment of assets, including CDs, to confirm that they were correctly classified for net capital purposes.
- **Agreement Review** – Obtaining from and verifying with banks the withdrawal terms of any assets, with particular focus on CD products, and reviewing all of the agreement terms, focusing on whether withdrawal restrictions may affect an asset's classification and its net capital charge for the terms of all assets, including CDs, and reviewing all of the agreement terms, focusing on whether withdrawal restrictions may affect an asset's classification and its net capital charge.
- **Training and Guidance** – Developing guidance and training for Financial and Operational Principal and other relevant staff on Net Capital Rule requirements for Fails, including how to report Fails on their balance sheets, track the age of Fails and if necessary, calculate any net capital deficit resulting from aged Fails.
- **Aging Review** – Performing reviews to confirm that they correctly aged Fail contract charges and correctly applied a net capital deduction, when applicable, to their net capital calculation.
- **Collaboration With Clearing Firms** – Clarifying WSPs to address clearing firms' responsibilities regarding net capital requirements, including for Fails, and introducing firms engaging their clearing firms to confirm that:
  - introducing firms were receiving a record of all Fails on a daily basis (or at least monthly);
  - clearing firms' reports included all of the required information; and
  - introducing firms were correctly interpreting the clearing firms' reports (especially distinctions between trade date and settlement date and those dates' implications for aging calculations for Fails).

Additional Resources

- **FASB**
  - **Revenue from Contracts with Customers (Topic 606)**
- FINRA
  - Funding and Liquidity Topic Page
  - **Interpretations to the SEC's Financial and Operational Rules**
  - ***Regulatory Notice 19-08*** **(Guidance on FOCUS Reporting for Operating Leases)**
  - *Regulatory Notice 15-33* (Guidance on Liquidity Risk Management Practices)
  - *Regulatory Notice 10-57* (Funding and Liquidity Risk Management Practices)
  - *Notice to Members 03-63* (SEC Issues Guidance on the Recording of Expenses and Liabilities by Broker/Dealers)

Liquidity Risk Management

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Effective liquidity controls are critical elements in a broker-dealer's risk management framework. Exchange Act Rule 17a-3(a)(23) requires firms that meet specified thresholds to make and keep current records documenting the credit, market and liquidity risk management controls established and maintained by the firm to assist it in analyzing and managing the risks associated with its business.

FINRA routinely reviews and has shared observations on firms' liquidity risk management practices, as discussed in *Regulatory Notice* 15-33 (Guidance on Liquidity Risk Management Practices) and *Regulatory Notice* 21-12 (FINRA Reminds Member Firms of Their Obligations Regarding Customer Order Handling, Margin Requirements and Effective Liquidity Management Practices During Extreme Market Conditions). Additionally, FINRA has adopted a new filing requirement—the Supplemental Liquidity Schedule—for firms with large customer and counterparty exposures. As noted in *Regulatory Notice* 21-31 (FINRA Establishes New Supplemental Liquidity Schedule (SLS)), the new SLS is designed to improve FINRA's ability to monitor for potential adverse changes in these firms' liquidity risk.

Related Considerations:

- What departments at your firm are responsible for liquidity management?
- How often does your firm review and adjust its assumptions regarding clearing deposits in its liquidity management plan and stress test framework?
- **Does your firm's liquidity management practices include processes for:**
  - **accessing liquidity during common stress conditions—such as increases in firm and client activities—as well as "black swan" events;**
  - **determining how the funding would be used; and**
  - **using empirical data from recent stress events to increase the robustness of its stress testing?**
- Does your firm's contingency funding plan take into consideration the amount of time needed to address margin calls from both customers and counterparties? Does your firm also take into consideration the type of transactions that are impacting the firm's liquidity?
- What kind of stress tests (*e.g.,* market or idiosyncratic) does your firm conduct? Do these tests include concentration limits within securities or sectors, and incorporate holdings across accounts held at other financial institutions?

Exam Observations and Effective Practices

Exam Observations:

- **Not Modifying Business Models** – Failing to incorporate the results of firms' stress tests into their business model.
- **Establishing Inaccurate Clearing Deposit Requirements – Incorrectly basing clearing deposit requirements on information that doesn't accurately represent their business operations (*e.g.,* using the amounts listed on FOCUS reports rather than spikes in deposit requirements that may have occurred on an intra-month basis).**
- **No Liquidity Contingency Plans** – Failing to develop contingency plans for operating in a stressed environment with specific steps to address certain stress conditions, including identifying the firm staff responsible for enacting the plan and the process for accessing liquidity during a stress event, as well as setting standards to determine how liquidity funding would be used.

Effective Practices:

- **Liquidity Risk Management Updates** – Updating liquidity risk management practices to take into account a firm's current business activities, including:
  - establishing governance around liquidity management, determining who is responsible for monitoring the firm's liquidity position, how often they monitor that position and how frequently they meet as a group; and
  - creating a liquidity management plan that considers:
    - quality of funding sources;
    - potential mismatches in duration between liquidity sources and uses;
    - potential losses of counterparties;
    - how the firm obtains funding in a business-as-usual condition and stressed conditions;
    - assumptions based on idiosyncratic and market-wide conditions;
    - early warning indicators and escalation procedures if risk limits are neared or breached; and
    - **material changes in market value of firm inventory over a short period of time.**
- **Stress Tests** – Conducting stress tests in a manner and frequency that consider the complexity and risk of the firm's business model, including:
  - assumptions specific to the firm's business (*e.g.,* increased haircuts on collateral pledged by firm, availability of funding from a parent firm) and based on historical data;
  - the firm's sources and uses of liquidity, and if these sources can realistically fund its uses in a stressed environment;
  - the potential impact of off-balance sheet items (*e.g.,* non-regular way settlement trades, forward contracts) on liquidity; and
  - periodic governance group review of stress tests.

Additional Resources

- ***Regulatory Notice* 21-31 (FINRA Establishes New Supplemental Liquidity Schedule (SLS))**
- ***Regulatory Notice* 21-12 (FINRA Reminds Member Firms of Their Obligations Regarding Customer Order Handling, Margin Requirements and Effective Liquidity Management Practices During Extreme Market Conditions)**
- *Regulatory Notice* 15-33 (Guidance on Liquidity Risk Management Practices)
- *Regulatory Notice* 10-57 (Funding and Liquidity Risk Management Practices)
- FINRA's Funding and Liquidity Topic Page

Credit Risk Management

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA has consistently reminded firms of the importance of properly managing credit risk and published *Notices* that offer guidance on effective funding and liquidity risk management practices (which are available in the "Additional Resources" section below). Risk exposures can arise from clearing arrangements, prime brokerage arrangements (especially fixed income prime brokerage), "give up" arrangements and sponsored access arrangements (discussed in the Market Access Rule section).

Further, firms should maintain a control framework where they manage credit risk and identify and address all relevant risks covering the extension of credit to their customers and counterparties. Weaknesses within the firm's risk management and control processes could result in a firm incorrectly capturing its exposure to credit risk. In particular, Exchange Act Rule 17a-3(a)(23) requires firms that meet specified thresholds to make and keep current records documenting the credit, market and liquidity risk management controls established and maintained by the firm to assist it in analyzing and managing the risks associated with its business.

Related Considerations:

- Does your firm maintain a robust internal control framework to capture, measure, aggregate, manage, supervise and report credit risk?
- Does your firm review whether it is accurately capturing its credit risk exposure, maintain approval and documented processes for increases or other changes to assigned credit limits, and monitor exposure to affiliated counterparties?
- Does your firm have a process to confirm it is managing the quality of collateral and monitoring for exposures that would have an impact on capital?

Exam Observations and Effective Practices

Exam Observations:

- **No Credit Risk Management Reviews** – Not evaluating firms' risk management and control processes to confirm whether they were accurately capturing their exposure to credit risk.
- **No Credit Limit Assignments** – Not maintaining approval and documentation processes for assignment, increases or other changes to credit limits.
- **No Monitoring Exposure** – Not monitoring exposure to firms' affiliated counterparties.

Effective Practices:

- **Credit Risk Framework** – Developing comprehensive internal control frameworks to capture, measure, aggregate, manage and report credit risk, including:
  - establishing house margin requirements;
  - identifying and assessing credit exposures in real-time environments;
  - issuing margin calls and margin extensions (and resolving unmet margin calls);
  - establishing the frequency and manner of stress testing for collateral held for margin loans and secured financing transactions; and
  - having a governance process for approving new, material margin loans.
- **Credit Risk Limit Changes** – Maintaining approval and documentation processes for increases or other changes to assigned credit limits, including:
  - having processes for monitoring limits established at inception and on an ongoing basis for customers and counterparties;
  - reviewing how customers and counterparties adhere to these credit limits and what happens if these credit limits are breached; and
  - maintaining a governance structure around credit limit approvals.

- **Counterparty Exposure** – Monitored exposure to affiliated counterparties, considering their:
  - creditworthiness;
  - liquidity and net worth;
  - track record of past performance (*e.g.,* traded products, regulatory history, past arbitration and litigation); and
  - internal risk controls.

Additional Resources

- *Regulatory Notice* 21-31 (FINRA Establishes New Supplemental Liquidity Schedule (SLS))
- *Regulatory Notice* 21-12 (FINRA Reminds Member Firms of Their Obligations Regarding Customer Order Handling, Margin Requirements and Effective Liquidity Management Practices During Extreme Market Conditions)
- FINRA's Funding and Liquidity Topic Page

Segregation of Assets and Customer Protection

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Exchange Act Rule 15c3-3 (Customer Protection Rule) imposes requirements on firms that are designed to protect customer funds and securities. Firms are obligated to maintain custody of customer securities and safeguard customer cash by segregating these assets from the firm's proprietary business activities and promptly delivering them to their owner upon request. Firms can satisfy this requirement by either keeping customer funds and securities in their physical possession or in a good control location that allows the firm to direct their movement (*e.g.,* a clearing corporation).

Related Considerations:

- What is your firm's process to prevent, identify, research and escalate new or increased deficits that are in violation of the Customer Protection Rule?
- What controls does your firm have in place to identify and monitor its possession or control deficits, including the creation, cause and resolution?
- If your firm claims an exemption from the Customer Protection Rule and it is required to forward customer checks promptly to your firm's clearing firm, how does your firm implement consistent processes for check forwarding and maintain accurate blotters to demonstrate that checks were forwarded in a timely manner?
- How does your firm train staff on Customer Protection Rule requirements?
- What are your firm's processes to confirm that your firm correctly completes its reserve formula calculation and maintains the amounts that must be deposited into the special reserve bank account(s)?
- If your firm is engaging in digital asset transactions, what controls and procedures has it established to assure compliance with the Customer Protection Rule? Has the firm analyzed these controls and procedures to address potential concerns arising from acting as a custodian (*i.e.,* holding or controlling customer property)?

Exam Findings and Effective Practices

Exam Findings:

- **Inconsistent Check-Forwarding Processes** – Not implementing consistent processes for check forwarding to comply with an exemption from the Customer Protection Rule.
- **Inaccurate Reserve Formula Calculations** – Failing to correctly complete reserve formula calculations due to errors in coding because of limited training and staff turnover, challenges with spreadsheet controls, limited coordination between various internal departments and gaps in reconciliation calculations.
- **Omitted or Inaccurate Blotter Information** – Maintaining blotters with insufficient information to demonstrate that checks were forwarded in a timely manner and inaccurate information about the status of checks.

Effective Practices:

- **Confirming Control Agreements** – Collaborating with legal and compliance departments to confirm that all agreements supporting control locations are finalized and executed before the accounts are established and coded as good control accounts on firms' books and records.
- **Addressing Conflicts of Interest** – Confirming which staff have system access to establish a new good control location and that they are independent from the business areas to avoid potential conflicts of interest; and conducting ongoing review to address emerging conflicts of interest.
- **Reviews and Exception Reports for Good Control Locations** – Conducting periodic review of and implementing exception reports for existing control locations for potential miscoding, out-of-date paperwork or inactivity.
- **Check-Forwarding Procedures** – Creating and implementing policies to address receipt of customer checks, checks written to the firm and checks written to a third party.
- **Check Forwarding Blotter Review** – Creating and reviewing firms' check received and forwarded blotters to confirm that they are up to date and include the information required to demonstrate compliance with the Customer Protection Rule exemption.

Additional Resources

- Customer Protection – Reserves and Custody of Securities (SEA Rule 15c3-3)
- U.S. Securities and Exchange Commission, Custody of Digital Asset Securities by Special Purpose Broker-Dealers, Exchange Act Release No. 34-90788 (Dec. 23, 2020)
- U.S. Securities and Exchange Commission, No-Action Letter to FINRA re: ATS Role in the Settlement of Digital Asset Security Trades (Sept. 25, 2020)

Portfolio Margin and Intraday Trading NEW FOR 2022

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA Rule 4210(g) (Margin Requirements) permits member firms to apply portfolio margin requirements—based on the composite risk of a portfolio's holdings—in margin accounts held by certain investors as an alternative to "strategy-based" margin requirements. Firms are required to monitor the risk of the positions held in these accounts during a specified range of possible market movements according to a comprehensive written risk methodology.

Related Consideration:

- Do the firm's policies and procedures for monitoring the risk of their investors' portfolio margin accounts comply with Rule 4210(g)(1), in particular:
  - maintaining a comprehensive written risk methodology for assessing the potential risk to the member's capital during a specified range of possible market movements of positions maintained in such accounts;
  - monitoring the credit risk exposure of portfolio margin accounts both intraday and end of day; and
  - maintaining a robust internal control framework reasonably designed to capture, measure, aggregate, manage, supervise and report credit risk exposure to portfolio margin accounts?

Exam Findings and Effective Practices

Exam Findings:

- **Inadequate Monitoring Systems** – Systems not designed to consistently identify credit risk exposure intra-day (*e.g.,* do not include defined risk parameters required to produce notifications or exceptions reports to senior management; require manual intervention to run effectively) or end of day (*e.g.,* cannot monitor transactions executed away in a timely manner).
- **Not Promptly Escalating Risk Exposures** – Staff failing to promptly identify and escalate incidents related to elevated risk exposure in portfolio margin accounts to senior management, in part due to insufficient expertise.
- **Insufficient WSPs** – Failing to maintain written supervisory procedures outlining intraday monitoring processes and controls.

Effective Practices:

- **Internal Risk Framework** – Developing and maintaining a robust internal risk framework to identify, monitor and aggregate risk exposure within individual portfolio margin accounts and across all portfolio margin accounts, including:
  - increasing house margin requirements during volatile markets in real-time;
  - conducting stress testing of client portfolios;
  - closely monitoring client fund portfolios' NAV, capital, profitability, client redemptions, liquidity, volatility and leverage to determine if higher margin requirements or management actions are required; and
  - monitoring and enforcing limits set by internal risk functions and considering trigger and termination events set forth in the agreement with each client.
- **Concentration Risk** – Maintaining and following reasonably designed processes (reflected in the firm's WSPs) and robust controls to monitor the credit exposure resulting from concentrated positions within both individual portfolio margin accounts and across all portfolio margin accounts, including processes to:
  - aggregate and monitor total exposure and liquidity risks with respect to accounts under common control;
  - identify security concentration at the aggregate and single account level; and
  - measure the impact of volatility risk at the individual security level.
- **Client Exposure** – Clearly and proactively communicating with clients with large or significantly increasing exposures, according to clearly delineated triggers and escalation channels established by the firm's WSPs; and requesting that clients provide their profit and loss position each month.

Additional Resource

- FINRA's Portfolio Margin FAQ

Appendix—Using FINRA Reports in Your Firm's Compliance Program

Firms have used prior FINRA publications, such as Exam Findings Reports and Priorities Letters (collectively, Reports), to enhance their compliance programs. We encourage firms to consider these practices, if relevant to their business model, and continue to provide feedback on how they use FINRA publications.

- **Assessment of Applicability** – Performed a comprehensive review of the findings, observations and effective practices, and identified those that are relevant to their businesses.
- **Risk Assessment** – Incorporated the topics highlighted in our Reports into their overall risk assessment process and paid special attention to those topics as they performed their compliance program review.
- **Gap Analysis** – Conducted a gap analysis to evaluate how their compliance programs and WSPs address the questions and effective practices noted in our Reports and determined whether their compliance programs have any gaps that could lead to the types of findings noted in those Reports.
- **Project Team** – Created interdisciplinary project teams and workstreams (with staff from operations, compliance, supervision, risk, business and legal departments, among other departments) to:
  - assign compliance stakeholders and project owners;
  - summarize current policies and control structures for each topic;
  - engage the legal department for additional guidance regarding regulatory obligations;
  - develop plans to address gaps; and
  - implement effective practices that were not already part of their compliance program.
- **Circulation to Compliance Groups** – Shared copies of the publications or summaries of relevant sections with their compliance departments.
- **Presentation to Business Leaders** – Presented to business leadership about their action plans to address questions, findings, observations and effective practices from our Reports.
- **Guidance** – Used Reports to prepare newsletters, internal knowledge-sharing sites or other notices for their staff.
- **Training** – Added questions, findings, observations and effective practices from Reports, as well as additional guidance from firms' policies and procedures, to their Firm Element and other firm training.

Endnotes

1. "Related Considerations" are intended to serve as a possible starting point in considering a firm's compliance program related to a topic. Firms should review relevant rules to understand the full scope of their obligations.
2. "Nesting" refers to FFIs indirectly gaining access to the U.S. financial system through another FFI's correspondent account at a U.S. financial institution. This practice can facilitate legitimate financial transactions, but member firms that maintain correspondent accounts with FFIs should have policies and procedures to identify and monitor for potentially illegitimate "nested" activity.
3. An IP address is a unique identifier assigned to an Internet-connected device, while a MAC is a unique identifier used to identify a specific hardware device at the network level.
4. *See Regulatory Notice 21-18* (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts)
5. *See Regulatory Notice 20-13* (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)
6. The SEC is proposing amendments to 17a-4 to allow for electronic records to be preserved in a manner that permits the recreation of an original record if it is altered, over-written, or erased. *See* the SEC's Proposed Rule: Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants.
7. These regulatory obligations stem from Exchange Act Rule 15c3-3(d)(4) and MSRB Rules G-17 and G-27 (for firm shorts), and MSRB Rule G12-(h) (for fails-to-receive).
8. Reg BI also applies to certain recommendations that were not previously covered under suitability obligations (*e.g.,* account recommendations, implicit hold recommendations in the case of agreed-upon account monitoring).
9. When a retail customer opens or has an existing account with a broker-dealer, the retail customer has a relationship with the broker-dealer and is therefore in a position to "use" the broker-dealer's recommendation.
10. While the SEC presumes that the use of the term "adviser" or "advisor" in a name or title by an associated person of a broker-dealer who is not also a supervised person of an investment adviser is a violation of the Disclosure Obligation under Reg BI, it recognizes that usage may be appropriate under certain circumstances. *See* FINRA's Reg BI and Form CRS Checklist for examples of possible exceptions.
11. *See* the SEC's December 17, 2021 Staff Statement Regarding Form CRS Disclosures for additional observations.
12. *Regulatory Notice 21-10* summarized the recent updates to the 5122/5123 Notification Filing Form that became effective on May 22, 2021, and *Regulatory Notice 21-26* announced that, as of October 1, 2021, FINRA Rules 5122 and 5123 require member firms to file retail communications that promote or recommend a private placement offering that is subject to these rules' filing requirements with FINRA's Corporate Financing Department.
13. *See* CAT NMS Plan, FAQ R.2 for the types of information firms should obtain from third-party vendors to satisfy these requirements.
14. *See, e.g., Regulatory Notice 21-23*.
15. In addition to the order routing disclosures under Rule 606, Rule 607 of Regulation NMS requires firms to disclose their policies regarding PFOF and order routing when customers open accounts, and on an annual basis thereafter, so firms should consistently provide the same information in both types of disclosures.
16. Firms are reminded that any affiliate obligated to pay firm expenses must have the independent financial means to satisfy those obligations.

www.finra.org

22_0021.1—02/22

Regulatory Notice 21-18

Cybersecurity

FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts

Summary

FINRA has received an increasing number of reports regarding customer account takeover (ATO) incidents, which involve bad actors using compromised customer information, such as login credentials (*i.e.,* username and password), to gain unauthorized entry to customers' online brokerage accounts.

To help firms prevent, detect and respond to such attacks, FINRA recently organized roundtable discussions with representatives from 20 firms of various sizes and business models to discuss their approaches to mitigating the risks from ATO attacks.

This *Notice* outlines the recent increase in ATO incidents; reiterates firms' regulatory obligations to protect customer information; and discusses common challenges firms identified in safeguarding customer accounts against ATO attacks, as well as practices they find effective in mitigating risks from ATOs—including recent innovations—which firms may consider for their cybersecurity programs.

This *Notice* does not create new legal or regulatory requirements, or new interpretations of existing requirements. A firm's cybersecurity program should be reasonably designed and tailored to the firm's risk profile, business model and scale of operations. There should be no inference that FINRA requires firms to implement any specific practices described in this *Notice*.

Questions regarding this *Notice* should be directed to:

- David Kelley, Director, Member Supervision Specialist Programs, at (816) 802-4729 or by email; or
- Greg Markovich, Senior Principal Risk Specialist, Member Supervision, at (312) 899-4604 or by email.

May 12, 2021

Notice Type

- Special Alert

Suggested Routing

- Compliance
- Information Technology
- Legal
- Operations
- Risk Management
- Senior Management

Key Topics

- Access Control
- Authentication
- Cybersecurity
- Fraud

Referenced Rules & Notices

- FINRA Rule 2090
- FINRA Rule 3110
- FINRA Rule 3310
- FINRA Rule 4512
- Information Notice 10/15/20
- Notice to Members 05-48
- Regulatory Notice 20-13
- Regulatory Notice 20-30
- Regulatory Notice 20-32

Background and Discussion

FINRA has received an increasing number of reports regarding ATO incidents, which involve bad actors using compromised customer information, such as login credentials, to gain unauthorized entry to customers' online brokerage accounts. In addition, we have received reports regarding attackers using synthetic identities to fraudulently open new accounts; some of the information addressed here, particularly regarding the opening of online accounts, may help firms mitigate risks in this area.[1]

Customer ATOs have been a recurring issue, but reports to FINRA about such attacks have increased as more firms offer online accounts, and more investors conduct transactions in these accounts, in part due to the proliferation of mobile devices and applications (*i.e.,* "apps")[2] and the reduced accessibility of firm's physical locations due to the COVID-19 pandemic.

Bad actors have taken advantage of these conditions to attempt customer ATOs, often through common attack methods such as phishing emails and social engineering attempts (*e.g.,* fraudsters calling customers, pretending to be registered representatives from customers' firms to acquire their personal information).[3] Other reasons for this increase in attempts may include the large number of stolen customer login credentials available for sale on the "dark web" (*see* Appendix for definitions of cybersecurity terms used in this *Notice*) and the emergence of more sophisticated ATO methods, such as tools that automate ATO attacks at scale (*e.g.,* using mobile emulators to mimic mobile devices that have been compromised to access thousands of online brokerage accounts).

Password Managers for Customer Account Protection

Some firms observed that customers often use the same login information across multiple accounts, making them particularly susceptible to ATOs conducted on a widescale (*e.g.,* credential stuffing).

To mitigate this threat, some firms recommend that customers use a password manager—an application that protects online accounts by suggesting and saving individual, strong passwords for each login. The password manager then automatically fills in the password whenever customers access their accounts online.

Regulatory Obligations

FINRA reminds member firms of their obligations to protect sensitive customer data, as well as verify the identity and know the essential facts concerning every customer:

Regulatory Obligation	Summary
FINRA Rule 2090 (Know Your Customer)	Firms must use reasonable diligence, in regard to the opening and maintenance of every account, to know the "essential facts" concerning every customer. Essential facts are those required to: (1) effectively service the customer's account; (2) act in accordance with any special handling instructions for the account; (3) understand the authority of each person acting on behalf of the customer; and (4) comply with applicable laws, rules and regulations.
SEC Regulation S-P, Rule 30	Firms must have written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information that are reasonably designed to ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of customer records and information; and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.
SEC Regulation S-ID	Firms must develop and implement a written program to detect, prevent and mitigate identity theft in connection with the opening or maintenance of "covered accounts."[4] In designing those programs, firms should consider, among other things, the methods of accessing covered accounts and the detection of red flags of identity theft in connection with authenticating customers.
Customer Identification Program (CIP)	Firms' anti-money laundering compliance programs must establish, document and maintain a written Customer Identification Program (CIP).[5] Among other requirements, firms' CIPs must include risk-based procedures that enable firms to form a reasonable belief that they know the true identity of each person that opens a new account. These procedures must be based on an assessment of the relevant risks, including those presented by the various types of accounts maintained by the firm and the various methods of opening accounts.[6] The CIPs must also describe when they will use documentary, non-documentary or a combination of both methods for identity verification.[7]

FINRA also encourages firms to assess their compliance programs related to new account openings and funds transfers, and review their policies and procedures related to:

- confirming that new account openings comply with FINRA Rule 4512 (Customer Account Information), as well as the Bank Secrecy Act and its implementing regulations addressed under FINRA Rule 3310 (Anti-Money Laundering Compliance Program);
- handling of ACH and other transmittal requests to "determine the authenticity of transmittal instructions" obligations pursuant to FINRA Rule 3110 (Supervision); and
- filing Suspicious Activity Reports (SARs)[8] with FinCEN.[9]

Common Challenges to Protecting Customer Accounts

During the roundtable discussions with FINRA, firms discussed the following cybersecurity challenges[10] they have encountered when safeguarding customer accounts from ATOs:

- identifying effective methods of verifying the identities of customers who establish accounts online;[11]
- addressing increased volume of attempted customer ATOs;
- preventing bad actors from transferring money in and out of customer accounts;
- identifying when bad actors have taken over customer accounts by modifying customers' critical account information (*e.g.,* email address, bank information) and are attempting fraudulent transactions;
- identifying when login attempts and requests to reset account passwords are actually made by a bad actor who has taken over a customer's email account; and
- balancing security and customer experience considerations.

Noted Practices

During the roundtable, firms discussed a variety of policies, procedures, controls and related tools to mitigate ATO-related risks. The firms typically used a risk-based approach to validating new customers' identities, authenticating logins to firm systems and performing customer-requested actions (*e.g.,* transactions in an account), coupled with strong back-end monitoring and robust procedures to respond quickly to identified customer ATOs.

Verifying Customers' Identities When Establishing Online Accounts

As part of their cybersecurity programs, firms that onboard customers online verified potential customers' identities by:

- validating identifying information or documents that applicants provide (*e.g.,* Social Security number (SSN), address, driver's license), including, for example, through "likeness checks"; and

- asking applicants follow-up questions or requesting additional documents to validate their identities, based on information from credit bureaus, credit reporting agencies or firms providing digital identity intelligence (*e.g.,* automobile and home purchases).

Alternatively, some firms contracted with third-party vendors to perform the above functions, as well as provide additional support (*e.g.,* a database to verify the legitimacy of suspicious information in customers' applications).[12]

Authenticating Customers' Identities During Login Attempts

Firms took a variety of approaches to validating the identities of customers when they access their online accounts:

Multifactor authentication: Most firms embraced multifactor authentication (MFA) as a key control that significantly reduces the likelihood that bad actors can take over a customer's account. Some of these firms required all customers to use MFA; others required customers to use MFA if their account had been compromised, while others simply encouraged customers to adopt it.

Key takeaway: *While not a "silver bullet," most participants believe MFA is currently one of the best ways to protect customers' accounts from ATOs.*

Unlike single-factor authentication (*e.g.,* a password), MFA uses two or more different types of factors or secrets—such as a password and code sent via a Short Message Service (SMS) text message or an authentication app—which significantly reduces the likelihood that the exposure of a single credential will result in account compromise.[13] A number of firms are encouraging customers to adopt MFA by establishing streamlined MFA methods, such as customers entering their login credentials on trusted devices.

Adaptive authentication: Some firms use adaptive authentication techniques to further increase the security of customers' accounts. Adaptive authentication typically assesses both:

- the risk associated with a customer's login (*i.e.,* the authentication system's confidence in the customer's identity, based on various factors associated with the login attempt (such factors are discussed further below)); and
- the risk of the activity the customer wishes to perform (*e.g.,* checking an account balance or initiating a money transfer).

In situations where the authentication system assesses that at least one of these risks exceeds a certain risk threshold, the system will require the customer to provide additional information to confirm their identity. For example, a customer may be required to provide additional information to verify their identity if they:

- attempt to log in to their account from a new device or different location than usual; or
- seek to execute a higher risk transaction such as an abnormally large withdrawal or purchase of a different type of security (*e.g.,* a low-priced unlisted security) than usual, or change a bank account or email address associated with their account.

A risk threshold can be set in a variety of ways. For example, a firm may set relatively simple rules (*e.g.,* transactions exceeding a specific dollar value or percent of account size). Alternatively, a firm may establish policies that assess a broad range of factors to determine whether additional verification is required.

Supplemental authentication factors: There are a variety of factors that firms and vendors may incorporate into their authentication system and processes to verify a customer's identity, including:

- SMS text message codes;
- phone call verifications;
- media access control (MAC) addresses;
- geolocation information;
- third-party authenticator apps; and
- biometrics.

In addition, many firms noted they have transitioned away from using email addresses as authentication factors, due to the prevalence of email account breaches by bad actors.

Back-End Monitoring and Controls

Firms conducted ongoing surveillance of both individual customer accounts and across these accounts to prevent, detect and mitigate ATO threats. (In some cases, the results of such back-end monitoring may feed back into firms' front-end controls.) This included, for example:

- monitoring at the customer account level for anomalies, such as:
  - indications of ATO attempts at the login level (*e.g.,* significant increases in number of failed logins in a brief time period for a specific account); and
  - account activity that could indicate that an ATO has occurred (*e.g.,* large purchases shortly after account opening; changes in email account of record followed by a request for a third-party wire; frequent transfers of funds in and out of an account);

- monitoring across customers' accounts for indications of credential stuffing or other large-scale attacks (*e.g.,* significant increases in the number of login attempts and failed logins across a large number of accounts);
- monitoring emails received from customers for red flags of social engineering (*e.g.,* problems with grammar or spelling; unexpected attachments, apps or links);[14]
- establishing back-end controls to prevent bad actors from moving money out of customer accounts, such as requiring a confirmation phone call with the customer using an established phone number when suspicious activity is detected in their account (*e.g.,* withdrawing money from an online brokerage account into a newly-established bank account); and
- scanning the dark web for keywords or data that could be useful to bad actors in facilitating an ATO (*e.g.,* firm name, customer account numbers, names of firm executives, planted accounts and passwords).

Procedures for Potential or Reported Customer ATOs

Firms discussed methods to proactively address potential or reported customer ATOs by:

- establishing a dedicated fraud group to investigate customer ATOs;
- responding promptly and effectively to customers who report ATOs, frequently updating them on their account status and minimizing the amount of time their accounts are locked or their trading ability is suspended;
- reviewing all of a customer's accounts at the firm for signs of problematic activity, if such activity is identified in one of their accounts;
- providing a method for customers to quickly communicate with someone at the firm, typically through voice or chat channels in a contact center; and
- reminding customers of recommended security practices (*e.g.,* MFA adoption).

Automated Threat Detection

Firms used a variety of automated processes to detect potential malicious actions by bad actors, for example, by:

- using web application firewalls (WAFs) and internally built tools to stop credential stuffing attacks;
- isolating suspicious IPs in a "penalty box"; and
- instituting geographic-based controls (*e.g.,* "impossible travel" or disallowing connections from countries where no customers reside).

Restoring Customer Account Access

Firms noted that secure practices to restore customers' account access—whether because a customer has forgotten their password or because they are otherwise locked out—in a timely fashion are essential. At the same time, however, the process must be well thought out and incorporate appropriate safeguards so that it does not itself become an avenue for ATOs. Practices firms noted in this regard included:

- implementing two-factor authentication for all password resets, for example, requiring input of a time-sensitive code sent to investors by SMS text message (several firms noted that sending a code via email can be risky because customers' email accounts may have been compromised, so firms using this approach may want to ask for additional confirming information, as described in the bullet below); and
- requiring customers to contact call centers, and answer security questions based on less commonly available information (*i.e.,* information less likely to be available through the dark web or a customer's social media posts, and provided by the credit bureaus or firms providing digital identity intelligence) to restore their account access.

Investor Education

Firms noted that they educated and trained their customers on account security by:

- including cybersecurity-related materials in the client onboarding process;
- providing up-to-date cybersecurity information;
- including on the firm's website resources—such as alerts—that customers can opt in to receiving, such as email or SMS text messages for certain types of account activity; and
- adding educational content to statements of older investors.

Reporting Fraud

FINRA urges firms to protect customers and other firms by immediately reporting scams and any other potential fraud to:

- FINRA's Regulatory Tip Form found on FINRA.org;
- U.S. Securities and Exchange Commission's tips, complaints and referral system (TCRs) or by phone at (202) 551-4790;
- the Federal Bureau of Investigation's (FBI) tip line at 800-CALLFBI (225-5324) or a local FBI office;
- the Internet Crime Compliant Center (IC3) for cyber-crimes (particularly if a firm is trying to recall a wire transfer to a destination outside the United States); and
- local state securities regulators.[15]

In addition, firms should consider whether circumstances require that the firm file a SAR[16] or report pursuant to FINRA Rule 4530 (Reporting Requirements).[17]

Conclusion

As noted herein, FINRA has received reports that the prevalence and sophistication of customer ATOs have been increasing. In the face of this threat, firms have implemented a variety of policies, procedures, controls and related tools to prevent, detect and respond to ATOs. FINRA shares practices roundtable participants found to be effective to help other firms mitigate ATO risks. Additional information related to cybersecurity risk management can be found on FINRA's Cybersecurity Topic Page.

Appendix

The following list defines commonly-used cybersecurity terms that appear in this *Notice*:

Biometrics – the unique physical identifiers (*e.g.,* fingerprint, voice and facial recognition) or behavioral characteristics (*e.g.,* mouse activity and keyboard strokes on computers; touchscreen behavior and device movement on mobile devices) humans display to digitally authenticate their identity.
Credential Stuffing – a cyberattack in which a bad actor uses a large set of illegally-acquired usernames and passwords to attempt to gain unauthorized access to multiple user accounts.
Dark Web – the portion of the Internet that can only be accessed through special types of software and is often used to anonymously conduct illegal activity.
Impossible Travel – a security control that compares the locations of a user's most recent two sign-in attempts to determine if travel between those locations was impossible in the timeframe given (*e.g.*, logging in from Cleveland, Ohio and then, twenty minutes later, from Salt Lake City, Utah).
Likeness Check – an identity verification method where applicants upload a photo or video of themselves, which is then compared with their recently submitted identity documents (and, at times, voice recordings).
Media Access Control (MAC) – a unique identifier used to identify a specific hardware device at the network level.
Penalty Box – a tool that isolates Internet Protocol (IP) addresses that exhibit potentially malicious behavior.
Planted Account – a fake account established by a firm within its customer database. In the context of cybersecurity, firms often monitor the dark web for information related to planted accounts to uncover data breaches.
Short Message Service (SMS) – a system for sending short messages (*e.g.,* text) over a wireless network.
Trusted Device – a device frequently used by a customer to access their online account, such as a mobile phone, tablet or home computer. A customer can designate a device as "trusted" on the Verification Code screen by clicking the box next to "Don't ask again on this computer".
Web Application Firewall (WAF) – a firewall that monitors traffic between a web application and the Internet and filters out any malicious traffic (as defined by its set of policies).

Endnotes

1. *See* Regulatory Notice 20-32 (FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud) for definitions of ATOs and synthetic identities.

2. *See* FINRA's 2018 Report on Selected Cybersecurity Practices for effective practices firms have implemented to protect sensitive firm and customer information as the use of mobile devices expands and becomes more widespread.

3. *See* Regulatory Notice 20-30 (Fraudsters Using Registered Representatives Names to Establish Imposter Websites).

4. *See* 17 CFR 248.201(b)(3), which defines "covered account" as:

   (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties; and

   (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

5. *See* 31 C.F.R. 1023.220 and 31 C.F.R. 1023.100(d). Pursuant to FINRA Rule 3310(b), firms must establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the Bank Secrecy Act and its implementing regulations, including the CIP Rule.

6. *Ibid.*

7. *See* 31 C.F.R. 1023.220(a)(2)(ii). For firms relying on documents to verify identity, the documents utilized may include an original unexpired government-issued identification evidencing nationality or residence and bearing a photograph, such as a driver's license or passport. Non-documentary methods of verifying customer identity under the CIP Rule may include contacting a customer; independently verifying the customer's identity through comparison of the information the customer provides with information from a consumer reporting agency, public database, or other source; checking references with other financial institution; or obtaining a financial statement.

8. *See* 31 C.F.R. 1023.320 for SARs reporting requirements.

9. *See* FinCEN's July 2020 Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic for additional guidance on filing SARs.

10. The challenges discussed in this *Notice* may require firms to address regulatory obligations beyond the context of cybersecurity—for example, those related to anti-money laundering compliance programs.

11. *See* FinCEN's July 2020 Advisory and *Regulatory Notice 20-13* (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic) for recent, common tactics bad actors use to establish fraudulent customer accounts.

12. Outsourcing an activity or function to a third party does not relieve firms of their ultimate responsibility for compliance with all applicable securities laws and regulations and FINRA and MSRB rules regarding the outsourced activity or function. FINRA has provided substantial guidance regarding firms' responsibilities when outsourcing activities to third-party service providers. *See, e.g.,* *Notice to Members 05-48* (Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers).

13. *See* *Information Notice 10/15/20* (Cybersecurity Background: Authentication Methods) for a primer on authentication techniques for firms to consider implementing within their cybersecurity programs.

14. *See* FINRA's 2018 Cybersecurity Report for additional effective practices firms have implemented to mitigate the threat of phishing attacks.

15. *See* North American Securities Administrations Association's Contact Your Regulator.

16. *See supra* note 9. *See also* FinCEN's Frequently Asked Questions (FAQs) regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through Suspicious Activity Reports (SARs).

17. For additional information about the requirements of FINRA Rule 4530 (Reporting Requirements), *see* Rule 4530 Frequently Asked Questions.