Vendor Management: Due Diligence and Oversight
Tuesday, May 17, 2022
8:30 a.m. – 9:30 a.m.

During this session, FINRA staff walk through various important considerations when choosing new vendors. Panelists discuss finding a technical solution that is a good fit for your firm, tips on performing an efficient due diligence review, contract issues, and advice on implementing the new software.

Moderator:
Kyle Morse
Vice President, Trading and Execution (T&E) Firm Examinations
FINRA Market Regulation

Panelists:
Catherine Dunn
Director, Capital Markets Firm Examinations
FINRA Member Supervision

Yuliana Landers
Manager, Retail Firm Examinations
FINRA Member Supervision

Matthew Reyburn
Director, Capital Markets Risk Monitoring
FINRA Member Supervision

Vendor Management: Due Diligence and Oversight Panelists Bios:

Moderator:

Kyle Morse, Vice President, Trading and Execution (T&E), currently manages examination teams for Market Regulation covering FINRA Firm Exams as well as Exchange RSA Sales Practice and T&E Fixed Income Trading Exams. Prior to assuming his role in the T&E examination program, Mr. Morse managed surveillance and investigative teams in Market Regulation for both Quality of Markets and Options Regulation. He has been with FINRA for 17 years and previously worked as a regulator for NYSE Arca, Pacific Stock Exchange and the Chicago Stock Exchange. Mr. Morse is currently the Executive Sponsor for the FINRA Women's Network. Outside of FINRA, Mr. Morse volunteers his time with the Cystic Fibrosis Foundation, serving as the President of the Corporate Advisory Board and Co-Chair of the Outreach and Advocacy Committee. Mr. Morse earned his B.A. from Illinois State University and his M.B.A in Financial Analysis from DePaul University.

Panelists:

Catherine Dunn is Examination Director in the Capital Markets Firm Examination Group within FINRA's Member Supervision Department. Ms. Dunn has been in this role since June 2020 and is based in the New Jersey Office. In this position, Ms. Dunn is responsible for leading a team of Examination Managers and Examiners who execute firm examinations. Ms. Dunn was an Examination Manager for 19 years in the New Jersey Office and has been associated with FINRA's Examination Program since joining FINRA in1999. Previously, Ms. Dunn worked at Merrill Lynch as a Senior Accountant in Financial Reporting and as an Auditor in the banking industry. Ms. Dunn has a B.S. in Accounting from Rutgers University.

Yuliana Landers is Examination Manger for FINRA's Member Supervision examination program. In this capacity, she has responsibility for managing a team that executes examinations of member firms who primarily service retail customers. Throughout her 10-year tenure at FINRA, Ms. Landers has held positions ranging from Compliance Examiner to Examination Manager. Ms. Landers began her career in Consumer and Small Business Banking with Wells Fargo Bank before obtaining her FINRA Series 7 and 66 licenses and transitioning to Wells Fargo Advisors. She received her Bachelor of Arts in Economics from Wartburg College and her Master of Science in Finance from University of Colorado. She is a member of the Association of Certified Anti-Money Laundering Specialists and serves as a Director for the Cancer League of Colorado Foundation.

Matt Reyburn is Risk Monitoring Director for the FINRA Capital Markets and Investment Banking firm grouping. During his 19 years with FINRA, he has served various roles as an Examiner and Examination Manager prior to becoming a Risk Monitoring Director. Mr. Reyburn's experience includes performing examination work through regulatory services agreements for the NASDAQ-LIFFE Single Stock Futures Exchange and Chicago Climate Exchange. As a Risk Monitoring Director, Mr. Reyburn and his team of analysts are responsible for performing the sales practice and financial/operational monitoring of approximately 270 Mergers and Acquisition broker-dealers located across the nation. Prior to joining FINRA, Mr. Reyburn performed various roles including Examination Manager and Strategic Development Analyst at the National Futures Association.

Vendor Management: Due Diligence and Oversight

Panelists

- **Moderator**
  - Kyle Morse, Vice President, Trading and Execution (T&E) Firm Examinations, FINRA Market Regulation
- **Panelists**
  - Catherine Dunn, Director, Capital Markets Firm Examinations, FINRA Member Supervision
  - Yuliana Landers, Manager, Retail Firm Examinations, FINRA Member Supervision
  - Matthew Reyburn, Director, Capital Markets Risk Monitoring, FINRA Member Supervision

To Access Polling

- **Please get your devices out:**
  - Type the polling address, **https://finra.cnf.io/sessions/ey7n** into the browser or scan the QR code with your camera.

  - Select your polling answers.

Polling Question 1

1. **Approximately how many services/functions does your firm outsource to a third-party?**
   a. 0
   b. 1-5
   c. 6-10
   d. 10+

Polling address: **https://finra.cnf.io/sessions/ey7n**

Polling Question 2

2. Approximately how many of your vendors does your firm maintain a written contract with?
   a. 0
   b. <25%
   c. 25-50%
   d. 50-75%
   e. 75%+

Polling address: **https://finra.cnf.io/sessions/ey7n**

Polling Question 3

3. **Is your off-boarding process documented in your firm's procedures and/or contracts with vendors?**
   a. Procedures
   b. Contracts
   c. Both
   d. Neither

Polling address: **https://finra.cnf.io/sessions/ey7n**

Regulatory Notice 21-29

Vendor Management and Outsourcing

FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors

Summary

Member firms are increasingly using third-party vendors to perform a wide range of core business and regulatory oversight functions. FINRA is publishing this *Notice* to remind member firms of their obligation to establish and maintain a supervisory system, including written supervisory procedures (WSPs), for any activities or functions performed by third-party vendors, including any sub-vendors (collectively, Vendors) that are reasonably designed to achieve compliance with applicable securities laws and regulations and with applicable FINRA rules. This *Notice* reiterates applicable regulatory obligations; summarizes recent trends in examination findings, observations and disciplinary actions; and provides questions member firms may consider when evaluating their systems, procedures and controls relating to Vendor management.

This *Notice*—including the "Questions for Consideration" below—does not create new legal or regulatory requirements or new interpretations of existing requirements. Many of the reports, tools or methods described herein reflect information firms have told FINRA they find useful in their Vendor management practices. FINRA recognizes that there is no one-size-fits-all approach to Vendor management and related compliance obligations, and that firms use risk-based approaches that may involve different levels of supervisory oversight, depending on the activity or function Vendors perform. Firms may consider the information in this *Notice* and employ the practices that are reasonably designed to achieve compliance with relevant regulatory obligations based on the firm's size and business model.

FINRA also notes that the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency recently published and requested comment on proposed guidance designed to help banking organizations manage risks associated with third-party relationships. FINRA will monitor this proposed guidance and consider comparable action, where appropriate.

August 13, 2021

Notice Type

- Guidance

Suggested Routing

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

Key Topics

- Business Continuity Planning (BCP)
- Cybersecurity
- Due Diligence
- Internal Controls
- Supervision
- Vendor Management

Referenced Rules & Notices

- FINRA Rule 1220
- FINRA Rule 3110
- FINRA Rule 4311
- FINRA Rule 4370
- Regulation S-P Rule 30
- Notice to Members 05-48

Questions or comments concerning this *Notice* may be directed to:

- Ursula Clay, Senior Vice President and Chief of Staff, Member Supervision, at 646-315-7375 or Ursula.Clay@finra.org;
- Sarah Kwak, Associate General Counsel, Office of General Counsel, at 202-728-8471 or Sarah.Kwak@finra.org;
- Michael MacPherson, Senior Advisor, Member Supervision, at 646-315-8449 or Michael.MacPherson@finra.org.

Background and Discussion

In 2005, FINRA published *Notice to Members 05-48* (Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers), which identified a number of common activities or functions that member firms frequently outsourced to Vendors, including "accounting/finance (payroll, expense account reporting, etc.), legal and compliance, information technology (IT), operations functions (*e.g.,* statement production, disaster recovery services, etc.) and administration functions (*e.g.,* human resources, internal audits, etc.)." Since that time, including during the COVID-19 pandemic, member firms have continued to expand the scope and depth of their use of technology and have increasingly leveraged Vendors to perform risk management functions and to assist in supervising sales and trading activity and customer communications.[1]

FINRA encourages firms that use—or are contemplating using—Vendors to review the following obligations and assess whether their supervisory procedures and controls for outsourced activities or functions are sufficient to maintain compliance with applicable rules.

CATEGORY	SUMMARY OF REGULATORY OBLIGATIONS
Supervision	FINRA Rule 3110 (Supervision) requires member firms to establish and maintain a system to supervise the activities of their associated persons that is reasonably designed to achieve compliance with federal securities laws and regulations, as well as FINRA rules, including maintaining written procedures to supervise the types of business in which it engages and the activities of its associated persons. This supervisory obligation extends to member firms' outsourcing of certain "covered activities"—activities or functions that, if performed directly by a member firm, would be required to be the subject of a supervisory system and WSPs pursuant to FINRA Rule 3110.[2] *Notice* 05-48 reminds member firms that "outsourcing an activity or function to ... [a Vendor] does not relieve members of their ultimate responsibility for compliance with all applicable federal securities laws and regulations and [FINRA] and MSRB rules regarding the outsourced activity or function." Further, *Notice* 05-48 states that if a member outsources certain activities, "the member's supervisory system and [WSPs] must include procedures regarding its outsourcing practices to ensure compliance with applicable securities laws and regulations and [FINRA] rules." FINRA expects member firms to develop reasonably designed supervisory systems appropriate to their business model and scale of operations that address technology governance-related risks, such as those inherent in firms' change and problem-management practices. Failure to do so can expose firms to operational failures that may compromise their ability to serve their customers or comply with a range of rules and regulations, including FINRA Rules 4370 (Business Continuity Plans and Emergency Contact Information), 3110 (Supervision) and books and records requirements under 4511 (General Requirements), as well as Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3 and 17a-4.

CATEGORY	SUMMARY OF REGULATORY OBLIGATIONS
Registration	*Notice* 05-48 reminds firms that, "in the absence of specific [FINRA] rules, MSRB rules, or federal securities laws or regulations that contemplate an arrangement between members and other registered broker-dealers with respect to such activities or functions (*e.g.,* clearing agreements executed pursuant to [FINRA Rule 4311]), any third-party service providers conducting activities or functions that require registration and qualification under [FINRA] rules will generally be considered associated persons of the member and be required to have all necessary registrations and qualifications." Accordingly, firms must review whether Vendors or their personnel meet any registration requirements under FINRA Rule 1220 (Registration Categories), as well as whether employees of the member firm are "Covered Persons" under the Operations Professional registration category pursuant to FINRA Rule 1220(b)(3), due to their supervision of "Covered Functions" executed by a Vendor or because they are authorized or have the discretion materially to commit the member firm's capital in direct furtherance of a Covered Function or to commit the member firm to any material contract or agreement (written or oral) with a Vendor in furtherance of a Covered Function.
Cybersecurity	SEC Regulation S-P Rule 30 requires broker-dealers to 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: (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. FINRA expects member firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations. FINRA reminds member firms to review core principles and effective practices for developing such programs and controls, including Vendor management, from our Report on Cybersecurity Practices (2015 Report) and the Report on Selected Cybersecurity Practices – 2018 (2018 Report), as well as other resources included in the Appendix to this *Notice*.

CATEGORY	SUMMARY OF REGULATORY OBLIGATIONS
Business Continuity Planning (BCP)	FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) requires member firms to create and maintain a written BCP with procedures that are reasonably designed to enable member firms to meet their existing obligations to customers, counterparties and other broker-dealers during an emergency or significant business disruption. The elements of each member firm's BCP—including their use of Vendors—can be "flexible and may be tailored to the size and needs of a member [firm]," provided that minimum enumerated elements are addressed. As a reminder, member firms must review and update their BCPs, if necessary, in light of changes to member firms' operations, structure, business or location.

Exam Findings and Observations

The 2021 Report on FINRA's Exam and Risk Monitoring Program, as well as our 2019, 2018 and 2017 Reports on FINRA Examination Findings, addressed compliance deficiencies (discussed below) arising from firms' Vendor relationships.

Cybersecurity and Technology Governance

- **Vendor Controls** – Firms failed to document or implement procedures to: 1) evaluate prospective and, as appropriate, test existing Vendors' cybersecurity controls, or 2) manage the lifecycle of their engagement with Vendors (*i.e.,* from onboarding, to ongoing monitoring, through off-boarding, including defining how Vendors dispose of customer non-public information).
- **Access Management** – Firms failed to implement effective Vendor access controls, including: limiting and tracking Vendors with administrator access to firm systems; instituting controls, such as a "policy of least privilege," to grant system and data access to Vendors only when required and removing access when no longer needed; or implementing multi-factor authentication for Vendors and contractors.
- **Inadequate Change Management Supervision** – Firms did not perform sufficient supervisory oversight of Vendors' application and technology changes impacting firm business and compliance processes, especially critical systems (including upgrades, modifications to or integration of member firm or Vendor systems). These oversight failures led to violations of regulatory obligations, such as those relating to data integrity, cybersecurity, books and records and confirmations.
- **Limited Testing of System Changes and Capacity** – Firms did not adequately test changes to, or system capacity of, order management, account access and trading algorithm systems, and thus failed to detect underlying malfunctions or capacity constraints.
- **Data Loss Prevention Programs** – Vendors did not encrypt confidential firm and customer data (*e.g.,* Social Security numbers) stored at Vendors or in transit between firms and Vendors.

FINRA Disciplined Firms Whose Vendors Did Not Implement Technical Controls

FINRA disciplined certain firms for violations of Regulation S-P Rule 30 and FINRA Rules 3110 and 2010 for failing to maintain adequate procedures and execute supervisory oversight to protect the confidentiality of their customers' nonpublic personal information, including, for example, where:

- a Vendor exposed to the public internet the firms' purchase and sales blotters, which included customers' nonpublic personal information (*e.g.,* names, account numbers, and social security numbers).
- a Vendor did not configure its cloud-based server correctly, install antivirus software, and implement encryption for the firm's account applications and other brokerage records containing customers' nonpublic personal information. As a result, foreign hackers successfully accessed the cloud-based server and exposed firm customers' nonpublic personal information.

Books and Records

- Firms failed to perform adequate due diligence to verify Vendors' ability to maintain books and records on behalf of member firms in compliance with Exchange Act Rules 17a-3 and 17a-4, as well as FINRA Rule 3110(b)(4) (Review of Correspondence and Internal Communications) and FINRA Rule Series 4510 (Books and Records Requirements) (collectively, Books and Records Rules).
- Firms failed to confirm that service contracts and agreements comply with requirements to provide notification to FINRA under Exchange Act Rule 17a-4(f)(2)(i), including a representation that the selected electronic storage media (ESM) used to maintain firms' books and records meets the conditions of Exchange Act Rule 17a-4(f)(2) and a third-party attestation as set forth in Exchange Act Rule 17a-4(f)(3)(vii) (collectively, ESM Notification Requirements).
- Firms did not confirm that Vendors complied with contractual and regulatory requirements to maintain (and not delete, unless otherwise permitted) firms' books and records.[3]

Consolidated Account Reports (CARs) – Firms did not have processes in place to evaluate how they and registered representatives selected CARs Vendors; set standards for whether and when registered representatives were authorized to use Vendor-provided CARs; determine when and how registered representatives could add manual entries or make changes to CARs; test or otherwise validate data for non-held assets reported in CARs (or clearly and prominently disclose that the information provided for those assets was unverified); and maintain records of CARs.[4]

Fixed Income Mark-up Disclosure – Firms failed to test whether Vendors identified the correct prevailing market price (PMP) from which to calculate mark-ups and mark-downs (for example, instead of using the prices of a member firm's own contemporaneous trades, which were available to be considered, a Vendor's program incorrectly identified PMPs using lower levels of the "waterfall" as described in FINRA Rule 2121.02 (Additional Mark-Up Policy For Transactions in Debt Securities, Except Municipal Securities) or MSRB Rule G-30.06 (Mark-Up Policy).

FINRA Disciplined Firms for Books and Records Violations Resulting from Vendor Deficiencies

FINRA disciplined firms for violations of Books and Records rules and related supervisory obligations involving Vendors, including, but not limited to, failing to preserve and produce business-related electronic communications (including emails, social media, texts, instant messages, app-based messages and video content) due to:

- Vendors' system malfunctions;
- Vendors' data purges after termination of their relationship with firms;
- Vendors failing to correctly configure default retention periods resulting in inadvertent deletions of firm electronic communication for certain time periods;
- Vendors' system configurations making deleted emails unrecoverable after 30 days;
- Vendors failing to provide non-rewriteable, non-erasable storage; and
- Firms failing to establish an audit system to account for Vendors' preservation of emails.

Questions for Consideration

The following questions may help firms evaluate whether their supervisory control system, including WSPs, adequately addresses issues and risks relating to Vendor management. The questions—which address both regulatory requirements and effective practices FINRA has observed firms implement—focus on four phases of a firm's outsourcing activities:

- deciding to outsource an activity or function,
- conducting due diligence on prospective Vendors,
- onboarding Vendors, and
- overseeing or supervising outsourced activities or functions.

As noted above, firms should not infer any new obligations from the questions for consideration. Many of the reports, tools or methods described herein reflect information firms have told FINRA they find useful in their vendor management practices. FINRA is sharing this information for firms' consideration only.

Firms may wish to evaluate the questions presented below in the context of a risk-based approach to Vendor management in which the breadth and depth of their due diligence and oversight may vary based on the activity or function outsourced to a Vendor. Factors firms may take into consideration include, but are not limited to:

- Will the Vendor be handling sensitive firm or customer non-public information?
- What would be the extent of the potential damage if there is a security breach (*e.g.,* number of customers or prospective customers impacted)?
- Is the Vendor performing a business-critical role or fulfilling a regulatory requirement for the firm?
- What is the reputation and history of the Vendor, including the representations made and information shared on how the Vendor will secure the firm's information?

I. Decision to Outsource

A decision to outsource an activity or function may depend, in part, on whether the firm has an adequate process to make that determination and then to supervise that outsourced activity or function. The following considerations may help firms address those threshold questions.

- Does your firm have a process for its decision-making on outsourcing, including the selection of Vendors?
- Does your firm's supervisory control system address your firm's outsourcing practices, including your firm's approach to Vendor due diligence?
- Does your firm identify risks that may arise from outsourcing a particular activity or function and consider the impact of such outsourcing on its ability to comply with federal securities laws and regulations, and FINRA rules?
- Does your firm engage key internal stakeholders (*e.g.,* Compliance, Legal, IT or Risk Management) relevant to, and with the requisite experience to assess, the outsourcing decision?

II. Due Diligence

Once a member firm decides to outsource an activity or function, it may want to consider some or all of the following questions in evaluating and selecting potential Vendors:

- Due Diligence Approach
  - What factors does your firm consider when conducting due diligence on potential Vendors? These may include, but are not limited to: a Vendors' financial condition, experience and reputation; familiarity with regulatory requirements, fee structure and incentives; the background of Vendors' principals, risk management programs, information security controls, and resilience.

- If a potential Vendor will be performing a function that is subject to regulatory requirements, how does your firm evaluate whether the Vendor has the ability to comply with applicable regulatory requirements and undertakings (*e.g.,* Book and Records rules, including ESM Notification Requirements)?
- Does your firm consider obtaining evaluations of prospective Vendors' SSAE 18, Type II, SOC 2 (System and Organization Control) reports (if available)? If so, who reviews the evaluations and how does your firm follow up on any identified concerns, including, for example, those related to cybersecurity?
- Does your firm take a risk-based approach to vendor due diligence? Does the scope and depth of your firm's due diligence reflect the degree of risk associated with the activities or functions that will be outsourced?
- Does your firm evaluate the impact to your customers or firm if a Vendor fails to perform, for example, by not fulfilling a regulatory obligation? What measures can your firm put in place to mitigate that risk?
- Does your firm assess the BCPs of prospective Vendors that would perform critical business, operational, risk management or regulatory activities or functions?
- If a Vendor will likely be conducting activities or functions that require registration under FINRA rules, does your firm have a process for determining whether the Vendor's personnel will be appropriately qualified and registered?
- Does your firm evaluate Vendors' controls and due diligence of Vendors' sub-contractors, particularly if the sub-contractor may have access to sensitive firm or customer non-public information or critical firm systems?
- Does your firm include individuals with the requisite expertise and experience in the due diligence process—including with respect to cybersecurity, information technology, risk management, business functions and relevant regulatory obligations—to effectively evaluate potential Vendors? How does your firm handle instances where your firm does not have the expertise or experience in-house?
- Does your firm document its due diligence findings?

- **Conflicts of Interest –** Does your firm put controls in place to mitigate potential conflicts of interest in the Vendor selection process? For example:
  - Does your firm require staff involved in its Vendor selection processes to disclose any personal relationship with the Vendor? If so, what steps does your firm take to assess whether that relationship may influence the choice of Vendor?
  - Does your firm allow staff to receive compensation or gifts from potential or current Vendors, which could influence the decision to select, or maintain a relationship with, a particular Vendor?

- **Cybersecurity**

Does your firm assess the Vendors' ability to protect sensitive firm and customer non-public information and data? Does your firm have access to expertise to conduct that assessment? (See also question, above, regarding SSAE 18 Type II, SOC 2 reports.)

III. Vendor Onboarding

After completing due diligence and selecting a Vendor, firms may wish to consider putting in place a written contract with the Vendor that addresses, among other things, both the firm's and the Vendor's roles with respect to outsourced regulatory obligations.

- **Vendor Contracts**
  - Does your firm document relationships with Vendors in a written contract, and if not, under what circumstances?
  - Do your firm's contracts address, when applicable, Vendors' obligations with respect to such issues as:
    - documentation evidencing responsible parties' and Vendors' compliance with federal and state securities laws and regulations and FINRA rules (*e.g.,* retention period required for preservation of firm records);
    - non-disclosure and confidentiality of information;
    - protection of non-public, confidential and sensitive firm and customer information;
    - ownership and disposition of firm and customer data at the end of the Vendor relationship;
    - notification to your firm of cybersecurity events and the Vendor's efforts to remediate those events, as well as notification of data integrity and service failure issues;
    - Vendor BCP practices and participation in your firm's BCP testing, including frequency and availability of test results;
    - disclosure of relevant pending or ongoing litigation;
    - relationships between Vendors, sub-contractors and other third-parties;
    - firm and regulator access to books and records; and
    - timely notification to your firm of application or system changes that will materially affect your firm.
  - Do your firm's contracts with Vendors address roles, responsibilities and performance expectations with respect to outsourced activities or functions?

- **Features and Default Settings of Vendor Tools**
  - Does your firm review, and as appropriate adjust, Vendor tool default features and settings, such as to limit use of communication tools to specific firm-approved features (*e.g.,* disabling a chat feature, or reviewing whether the communications are being captured for supervisory review), to set the appropriate retention period for data stored on a vendor platform or to limit data access—to meet your firm's business needs and applicable regulatory obligations?

IV. Supervision

Member firms have a continuing responsibility to oversee, supervise and monitor the Vendor's performance of the outsourced activity or function. Firms may wish to consider the following potential steps in determining how they fulfill this supervisory obligation:

- Obtaining representations from the Vendor in a contractual agreement that they are conducting self-assessments and undertaking the specific responsibilities identified;
- Requiring Vendors to provide attestations or certifications that they have fulfilled certain reviews or obligations;
- Going onsite to Vendors to conduct testing or observation, depending on the firm's familiarity with the vendor or other risk-based factors;
- Monitoring and assessing the accuracy and quality of the Vendor's work product;
- Remaining aware of news of Vendor deficiencies and investigating whether they are indicative of a problem with an activity or function the Vendor is performing for your firm;
- Investigating customer complaints that may be indicative of issues with a Vendor and exploring whether there are further-reaching impacts; and
- Training staff to address and escalate red flags at your firm that a Vendor may not be performing an activity or function adequately, such as not receiving confirmation that a Vendor task was completed.

In addition to the above, firms may want to consider asking the following questions, where applicable, with respect to more specific aspects of their supervisory system.

- **Supervisory Control System**
  - Does your firm monitor Vendors (for example, by reviewing SOC 2 reports) and document results of its ongoing supervision, especially for critical business or regulatory activities or functions?
  - Do your firm's WSPs address roles and responsibilities for firm staff who supervise Vendor activities?
  - Does your firm periodically review and update its Vendor management-related WSPs to reflect material changes in the firm's business or business practices?

- **Business Continuity Planning**
  - Does your firm's business continuity planning and testing include Vendors? If so, what are the testing requirements for Vendors and how often are such tests performed? How do these tests inform your firm's overall BCP?
  - Does your firm have contingency plans for interruptions or terminations of Vendor services?
  - If there is a disaster recovery event, has your firm assessed whether the Vendor will have sufficient staff dedicated to your firm?
- **Cybersecurity and Technology Change Controls**
  - **Access Controls**
    - Does your firm know which Vendors have access to: (1) sensitive firm or customer non-public information and (2) critical firm systems?
    - Does your firm implement access controls through the lifecycle of its engagement with Vendors, including developing a "policy of least privilege" to grant Vendors system and data access only when required and revoke it when no longer needed and upon termination?
    - Has your firm considered implementing multi-factor authentication for Vendors and, if warranted, their sub-contractors?
  - **Cybersecurity Events and Data Breaches**
    - Does your firm conduct independent, risk-based reviews to determine if Vendors have experienced any cybersecurity events, data breaches or other security incidents? If so, does your firm evaluate the Vendors' response to such events?
    - If a cybersecurity breach occurred at your firm's Vendor, was your firm notified and, if so, how quickly? Did your firm follow its incident response plan for addressing such breaches?
  - **Technology Change Management**
    - If applicable, how does your firm become aware of, evaluate and, as appropriate, test the impact of changes Vendors make to their applications and systems, especially for critical applications and systems?

FINRA Disciplined Firms for Failure to Supervise Vendors

FINRA disciplined certain firms that violated FINRA Rules 2010 and 3110, among other rules, when they failed to establish and maintain supervisory procedures for their Vendor arrangements reasonably designed to:

- Review, verify or correct vendor-provided expense ratio and historical performance information for numerous investment options in defined contribution plans (*i.e.,* retirement plans), causing firms' customer communications to violate FINRA Rule 2210;
- Oversee, monitor and evaluate changes and upgrades to automated rebalancing and fee allocation functions outsourced to a Vendor for wealth management accounts custodied at the firm, causing errors and imposing additional fees to customer accounts;
- Review, test or verify the accuracy and completeness of data feeds from Vendors that failed to identify the firm's prior role in transactions for issuers covered by firm research reports, resulting in violations of then NASD Rule 2711(h) and 2241(c) when the firm failed to make required disclosures in its equity research reports regarding its status as a manager or a co-manager of a public offering of the issuer's equity securities; and
- Confirm the accuracy and completeness of information provided by Vendors to regulators, including FINRA, both in response to specific requests and as part of regular trade and other reporting obligations, causing inaccurate responses and misreported transactions, order reports, route reports and reportable order events.

Conclusion

As noted throughout this *Notice*, the requirement that a member firm maintain a reasonably designed supervisory system and associated WSPs extends to activities or functions it may outsource to a Vendor. While the manner and frequency by which these activities or functions are overseen is determined by the member firm, and is dependent on a number of factors, the information in this *Notice* is intended to provide firms with ideas and questions they can use to build and evaluate the sufficiency of their Vendor management protocols. Additional helpful resources can be found in the Appendix.

Endnotes

1. *See Regulatory Notice* 20-42 (FINRA Seeks Comment on Lessons from the COVID-19 Pandemic); COVID-19/Coronavirus Topic Page; *Regulatory Notice* 20-16 (FINRA Shares Practices Implemented by Firms to Transition to, and Supervise in, a Remote Work Environment During the COVID-19 Pandemic); and *Regulatory Notice* 20-08 (Pandemic-Related Business Continuity Planning, Guidance and Relief).

2. *See also* NASD Office of General Counsel, Regulatory Policy and Oversight Interpretive Guidance, which clarified that *Notice 05-48* was issued to provide guidance on a member's responsibilities if the member outsources certain activities and was not intended to address the appropriateness of outsourcing a particular activity or whether an activity could be outsourced to a non-broker-dealer third-party service provider.

3. *See Regulatory Notice* 18-31 (SEC Staff Issues Guidance on Third-Party Recordkeeping Services).

4. *See Regulatory Notice* 10-19 (FINRA Reminds Firms of Responsibilities When Providing Customers with Consolidated Financial Account Reports).

Appendix – Additional Resources

Regulatory Notices and Guidance

- **Outsourcing and Vendor Management**
  - *Regulatory Notice* 11-14 (FINRA Requests Comment on Proposed New FINRA Rule 3190 to Clarify the Scope of a Firm's Obligations and Supervisory Responsibilities for Functions or Activities Outsourced to a Third-Party Service Provider)
  - *Notice to Members* 05-48 (Members' Responsibilities When Outsourcing Activities to Third-Party Providers), and NASD Office of General Counsel, Regulatory Policy and Oversight Interpretive Guidance
  - *Regulatory Notice* 18-31 (SEC Staff Issues Guidance on Third-Party Recordkeeping Services)
- **Cybersecurity**
  - Report on Selected Cybersecurity Practices – 2018
  - Report on Cybersecurity Practices – 2015

FINRA Examination Findings Reports

- 2021 Report on FINRA's Examination and Risk Monitoring Program
- 2019 Report on FINRA Examination Findings and Observations
- 2018 Report on FINRA Examination Findings
- 2017 Report on FINRA Examination Findings

Tools

- Core Cybersecurity Controls for Small Firms
- Small Firm Cybersecurity Checklist
- Outsourcing and Vendor Management section of the Peer-2-Peer Compliance Library
  - Outsourcing Due Diligence Form
  - Sample Vendor On-Site Audit Template
  - Sample Vendor Questionnaire
  - Third Party Matrix
  - Third Party Vendor Contracts Sample Language
  - Vendor Management Considerations
  - Vendor Security Questionnaire

Notice to Members

JULY 2005

SUGGESTED ROUTING

Legal and Compliance
Operations
Senior Management

KEY TOPICS

Due Diligence
Outsourcing
Supervisory Responsibilities
Third-Party Service Providers

GUIDANCE

Outsourcing

Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers

Executive Summary

NASD is aware that members are increasingly contracting with third-party service providers to perform certain activities and functions related to their business operations and regulatory responsibilities that members would otherwise perform themselves—a practice commonly referred to as outsourcing. NASD is issuing this *Notice* to remind members that, in general, any parties conducting activities or functions that require registration under NASD rules will be considered associated persons of the member, absent the service provider separately being registered as a broker-dealer and such arrangements being contemplated by NASD rules (such as in the case of clearing arrangements), MSRB rules, or applicable federal securities laws or regulations. In addition, outsourcing an activity or function to a third party does not relieve members of their ultimate responsibility for compliance with all applicable federal securities laws and regulations and NASD and MSRB rules regarding the outsourced activity or function. As such, members may need to adjust their supervisory structure to ensure that an appropriately qualified person monitors the arrangement. This includes conducting a due diligence analysis of the third-party service provider.

Questions/Further Information

Questions or comments concerning this *Notice* may be directed to Patricia Albrecht, Assistant General Counsel, Office of General Counsel, Regulatory Policy and Oversight, at (202) 728-8026.

Background

The practice of contracting with third-party service providers/vendors to perform certain activities and functions on a continuing basis (outsourcing) is not new to the securities industry. For example, NASD Rule 3230 (Clearing Agreements) has long permitted members that are introducing broker-dealers to enter into contracts with registered clearing broker-dealers that allocate certain functions and responsibilities, such as providing execution services, custody, and margin; maintaining books and records; and receiving, delivering, and safeguarding funds. Over the years, however, members' outsourcing activities have grown beyond the use of clearing agreements. Now, members regularly enter into outsourcing arrangements with entities other than broker-dealers. These entities may be unregulated, such as providers of data services, or regulated, such as transfer agents. Additionally, members increasingly are outsourcing activities other than those traditionally performed pursuant to clearing agreements.

To better understand their members' outsourcing activities, NASD and the New York Stock Exchange (NYSE) conducted a joint survey in October 2004 of a select number of broker-dealers. The survey sought to determine whether broker-dealers had procedures in place to determine the proficiency of service providers, whether outsourced business functions were properly monitored, and whether broker-dealers were in compliance with applicable regulations pertaining to the privacy of customer information in connection with such outsourcing arrangements. The survey found that, in many instances, there was a lack of written procedures to monitor the outsourcing of services, a lack of business continuity plans on the part of service providers and members with respect to outsourced services, and a lack of formalized due diligence processes to screen service providers for proficiency. However, while not always in the form of written procedures, most participants reported that they did have methods that they used to monitor and assess a third-party vendor's own procedures and performance and the accuracy and quality of the work product produced on a continuing basis. These methods included (1) using programmatic checks through business operations; (2) including the procedures in the contracts with the vendors; (3) requiring status reports and periodic meetings; and (4) testing and reviewing the third parties' procedures.

The survey results also provided a snapshot of the type and range of activities being outsourced and the nature of the third-party service providers being used. Survey participants frequently outsourced functions associated with accounting/finance (payroll, expense account reporting, etc.), legal and compliance, information technology (IT), operations functions (*e.g.*, statement production, disaster recovery services, etc.), and administration functions (*e.g.*, human resources, internal audits, etc.). Approximately two-thirds of the third-party vendors used by survey participants were regulated entities, subject to the jurisdiction of the Securities and Exchange Commission, NASD, NYSE, the Board of Governors of the Federal Reserve System, and/or the Office of the Comptroller of the Currency. The remaining third-party vendors were unregulated entities—both foreign and domestic. Survey participants indicated that they used foreign third-party vendors most often when outsourcing IT and communications activities.[1]

Discussion

Given the growing trend among members to outsource an increasing number of activities and functions to outside entities—both regulated and unregulated—and the lack of uniformity in members' procedures regarding members' use of outsourcing, NASD is issuing this *Notice* to provide guidance on requirements that pertain to the outsourcing of activities and functions that, if performed directly by members, would be required to be the subject of a supervisory system and written supervisory procedures pursuant to Rule 3010 (covered activities).[2] In addition, members are reminded that, in the absence of specific NASD rules, MSRB rules, or federal securities laws or regulations that contemplate an arrangement between members and other registered broker-dealers with respect to such activities or functions (*e.g.*, clearing agreements executed pursuant to NASD Rule 3230), any third-party service providers conducting activities or functions that require registration and qualification under NASD rules will generally be considered associated persons of the member and be required to have all necessary registrations and qualifications.

I. Accountability and Supervisory Responsibility for Outsourced Functions

Rule 3010 requires NASD members to design a supervisory system and corresponding written supervisory procedures that are appropriately tailored to each member's business structure.[3] If a member, as part of its business structure, outsources covered activities, the member's supervisory system and written supervisory procedures must include procedures regarding its outsourcing practices to ensure compliance with applicable securities laws and regulations and NASD rules. The procedures should include, without limitation, a due diligence analysis of all of its current or prospective third-party service providers to determine whether they are capable of performing the outsourced activities.[4]

After the member has selected a third-party service provider, the member has a continuing responsibility to oversee, supervise, and monitor the service provider's performance of covered activities. This requires the member to have in place specific policies and procedures that will monitor the service providers' compliance with the terms of any agreements and assess the service provider's continued fitness and ability to perform the covered activities being outsourced. Additionally, the member should ensure that NASD and all other applicable regulators have the same complete access to the service provider's work product for the member, as would be the case if the covered activities had been performed directly by the member.

Members should also include specific policies and procedures to determine whether any covered activities that the member is contemplating outsourcing are appropriate for outsourcing. To determine the appropriateness of outsourcing a particular activity, firms may want to consider certain factors, such as the financial, reputational, and operational impact on the member firm if the third-party service provider fails to perform; the potential impact of outsourcing on the member's provision of adequate services to its customers; and the impact of outsourcing the activity on the ability and capacity of the member to conform with regulatory requirements and changes in requirements.[5] These factors, however, are not meant to illustrate all of the factors a member may want to consider and are not meant to be an exclusive or exhaustive list of factors a member may need to consider.

In addition, members are reminded that outsourcing covered activities in no way diminishes a member's responsibility for either its performance or its full compliance with all applicable federal securities laws and regulations, and NASD and MSRB rules.

II. Activities and Functions that are Prohibited from being Outsourced

A. Activities and Functions Requiring Registration and Qualification

It is NASD's view that the performance of covered activities, which require qualification and registration, cannot be deemed to have been outsourced because the person performing the activity is an associated person of the member irrespective of whether such person is registered with the member. An exception would be where a third-party service provider is separately registered as a broker-dealer and the contracted arrangement between the member and the service provider is contemplated by NASD rules, MSRB rules, or applicable federal securities laws or regulations.[6] An example of such an exception would be a clearing agreement executed pursuant to NASD Rule 3230 between a member and a clearing broker-dealer.[7]

B. Supervisory and Compliance Activities

NASD has noted in previous guidance that the ultimate responsibility for supervision lies with the member.[8] Accordingly, a member may never contract its supervisory and compliance activities away from its direct control. This prohibition, however, does not preclude a member from outsourcing certain activities that support the performance of its supervisory and compliance responsibilities. For example, a member may implement a supervisory system designed by another party, which could include a computer software program that detects excessive trading in customer accounts. However, if a member chooses to implement such a system, it must make its own determination that the system implemented is current and reasonably designed to achieve compliance as required under Rule 3010. This may include, for example, monitoring the system to ensure that it functions as designed and that such design is of an adequate nature and breadth.[9]

Endnotes

1 A February 2005 joint report by the Joint Forum of the Basel Committee on Banking Supervision found similar trends in the use of outsourcing by financial firms. *See Outsourcing in Financial Services*, The Joint Forum of the Basel Committee on Banking Supervision (February 2005). The Joint Forum was established in 1996 under the aegis of the Basel Committee on Banking Supervision (Basel Committee), the International Organization of Securities Commissions (IOSCO), and the International Association of Insurance Supervisors (IAIS) to address issues common to the banking, securities, and insurance sectors, including the regulation of financial conglomerates. The Joint Forum is composed of an equal number of senior bank, insurance, and securities supervisors representing each supervisory constituency.

2 Examples of covered activities include, without limitation, order taking, handling of customer funds and securities, and supervisory responsibilities under Rules 3010 and 3012.

3 *See* Rule 3010(a) and (b); *Notice to Members (NTM) 99-45* (June 1999).

4 Rule 3012 also requires a member firm to have a written supervisory control system that will, among other things, test and verify that the member's supervisory policies and procedures are reasonably designed to achieve compliance with the applicable securities laws and regulations and NASD rules. Members are reminded that this requirement includes the testing and verification of their supervisory procedures regarding their outsourcing practices, including testing and verifying that any due diligence procedures meet the "reasonably designed to achieve compliance" standard. *See NTM 99-45* (June 1999) (providing guidance on the meaning of the term "reasonably designed to achieve compliance"). Such testing and verifying will help firms to ensure that their due diligence analyses of third-party service providers remain current and relevant.

5 Members may also want to consult a February 2005 IOSCO report for more factors that they should consider in connection with outsourcing. *See Principles of Outsourcing of Financial Services for Market Intermediaries*, IOSCO Technical Committee (February 2005). Another resource members may want to consider is the previously mentioned report by the Joint Forum of the Basel Committee on Banking Supervision. *Outsourcing in Financial Services, supra* note 1.

6 NASD does not view a third-party vendor as an associated person of the member if it solely provides services such as a trade execution and reporting system or automated data services in connection with back-office functions that, in turn, are utilized by registered or other associated persons of the member.

7 *See* Rule 3230(a)(1). Some members also enter into secondary or sub-clearing (sometimes referred to as "piggyback clearing") arrangements for clearing services with an intermediary firm that has an existing contract with a clearing firm instead of contracting directly with the clearing firm. Because intermediary firms do not always identify to clearing firms which accounts belong to the piggybacking firms, NASD has filed with the SEC a proposed rule change to Rule 3230 and Rule 3150 (Reporting Requirements for Clearing Firms) that would require intermediary firms to identify the accounts belonging to the piggybacking firms and that would require clearing firms to distinguish the data belonging to intermediary firms from the data belonging to the piggybacking firms.

8 *See NTM 99-45* (June 1999).

9 *See id.*

Remote Supervision
Tuesday, May 17, 2022
8:30 a.m. – 9:30 a.m.

Join FINRA staff and industry panelists as they discuss what they have learned from working remotely. During the session, panelists discuss effective controls, procedures, and processes that member firms are incorporating to address supervision in a remote work environment.

Moderator:
Shelly Davis
Director, Retail Risk Monitoring
FINRA Member Supervision

Panelists:
Sarah Kwak
Associate General Counsel, Regulatory
FINRA Office of General Counsel

Jessica Pastorino
President and Chief Compliance Officer
M&A Securities Group, Inc.

Gina Rettagliata
Director, Retail Firm Examinations
FINRA Member Supervision

Remote Supervision Panelists Bios:

Moderator:

Shelly Davis is Risk Monitoring Director with the Financial Industry Regulatory Authority, where she currently manages Risk Monitoring Analysts who focus on Retail Private Placements and Public Pooled Investment Vehicles. In this capacity, she is responsible a team of analysts and works to identify and address current and emerging risks at member firms. Ms. Davis has worked in the industry for over 23 years in various departments in the Nasdaq Stock Market and NASD/FINRA in Washington, DC, New York City, and New Jersey. Ms. Davis has a bachelor's degree from Wellesley College and is registered Certified Fraud Examiner with the ACFE.

Panelists:

Sarah S. Kwak is Associate General Counsel in FINRA's Office of General Counsel, specializing in sales practice regulatory policy with a particular focus on the FINRA rules governing the membership application process, supervision, and customer account statements. Prior to joining FINRA, Ms. Kwak was an Assistant Vice President at Merrill Lynch Pierce Fenner & Smith and served as a judicial law clerk for United States Bankruptcy Court Judge Barry Russell of the Central District of California. She holds two bachelor's degrees from the University of California at Irvine and a J.D. from Washburn University School of Law.

Jessica Pastorino has worked in the securities industry since 2006, managing compliance for firms involved in privately placed capital raising and M&A advisory. As President and Chief Compliance Officer for M&A Securities Group and Burch & Company, Ms. Pastorino runs two firms that offers a broker-dealer platform for independent middle-market investment banking professionals and boutique advisory groups. Ms. Pastorino holds her Series 24, 79, 62, 22, 39 and 63 licenses and earned her Bachelor of Arts Degree in English at California State University Long Beach. Ms. Pastorino has served as a member of both FINRA's District and Capital Acquisition Broker committees and currently serves on FINRA's Small Firm Advisory Committee.

Gina Rettagliata joined FINRA in 2003 and is Examination Director located in the Woodbridge, New Jersey office. She leads a geographically dispersed team of Exam Managers responsible for planning and executing Member Supervision's examination program relative to a subset of firms engaged primarily in retail sales. She brings several years of industry experience to her role, including as Vice President and AML Compliance Officer of a major online trading firm. Mrs. Rettagliata has a Bachelor of Arts degree in Political Science from the University of South Florida and is a graduate of the FINRA Institute at Georgetown Certified Regulatory and Compliance Professional (CRCP)® program.

Remote Supervision

Panelists

- **Moderator**
  - Shelly Davis, Director, Retail Risk Monitoring, FINRA Member Supervision
- **Panelists**
  - Sarah Kwak, Associate General Counsel, Regulatory, FINRA Office of General Counsel
  - Jessica Pastorino, President and Chief Compliance Officer, M&A Securities Group, Inc.
  - Gina Rettagliata, Director, Retail Firm Examinations, FINRA Member Supervision

Agenda

- Introduction
- Panel Discussion
- Poll
- Panel Q&A
- Poll
- Audience Q&A

Topic #1 – Panel Discussion

To Access Polling

- **Please get your devices out:**
  - Type the polling address, **https://finra.cnf.io/sessions/tfxe** into the browser or scan the QR code with your camera.

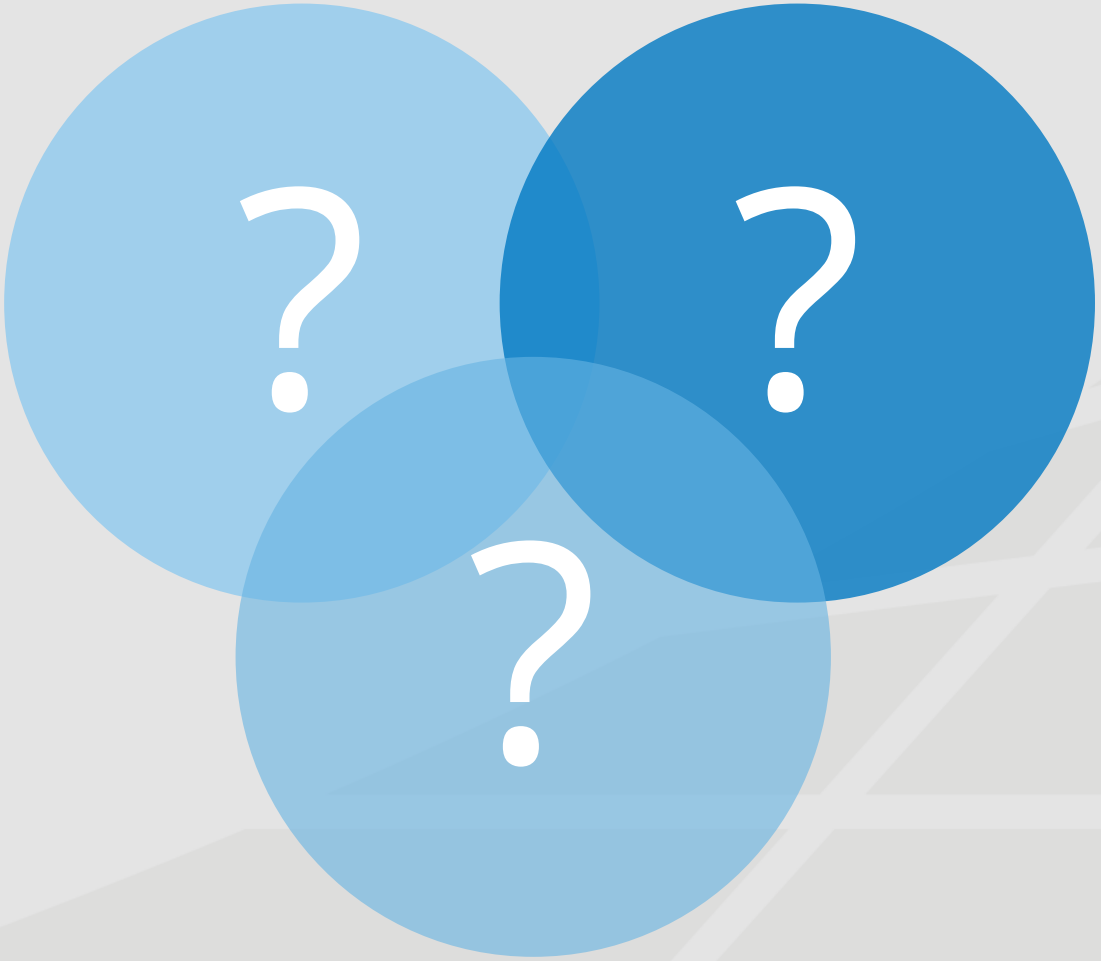
  - Select your polling answers.

Polling Question 1

1. **Coffee Talk: How do you prefer your coffee?**
   a. French Press
   b. Percolate
   c. Neither – tea for me

Polling address: **https://finra.cnf.io/sessions/tfxe**

Panel Q&A



Topic #2 – Panel Discussion

Polling Question 2

2. In how many time zones do you supervise? (Hawaiian-Aleutian, Alaska, Pacific, Mountain, Central, Eastern)
   a. One
   b. Two
   c. Three
   d. Four
   e. Five
   f. Six

Polling address: **https://finra.cnf.io/sessions/tfxe**

Topic #3 – Panel Discussion

Topic #4 – Panel Discussion

Audience Questions

Remote Supervision
Tuesday, May 17, 2022
8:30 a.m. – 9:30 a.m.

Resources:

- FINRA *Regulatory Notice 21-44*, *Business Continuity Planning and Lessons From the COVID-19 Pandemic* (December 2021)

  www.finra.org/rules-guidance/notices/21-44

- FINRA *Regulatory Notice 20-16, FINRA Shares Practices Implemented by Firms to Transition to, and Supervise in, a Remote Work Environment During the COVID-19 Pandemic* (May 2020)

  www.finra.org/rules-guidance/notices/20-16

- FINRA *Regulatory Notice 20-13 FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic (*May 2020*)*

  www.finra.org/rules-guidance/notices/20-13

- FINRA Proposed Rule Change to Adopt Temporary Supplementary Material .17 (Temporary Relief to Allow Remote Inspections for Calendar Year 2020 and Calendar Year 2021) under FINRA Rule 3110 (Supervision).

  www.finra.org/rules-guidance/rule-filings/sr-finra-2020-040

- *2022 Report on FINRA's Examination and Risk Monitoring Program* (February 2022)

  www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program

- SEC *2022 Examination Priorities Report, Division of Examinations*

  www.sec.gov/files/2022-exam-priorities.pdf

- NASAA 2018 Broker-Dealer Section Coordinated Examination Report on Findings and Recommended Best Practices

  www.nasaa.org/wp-content/uploads/2018/09/BD-Coordinated-Examination-Report-2018.pdf

Options
Tuesday, May 17, 2022
8:30 a.m. – 9:30 a.m.

Join FINRA staff and industry panelists as they discuss regulatory issues impacting options markets.

Moderator:

Gene DeMaio
Executive Vice President, Options Regulation and T&E
FINRA Market Regulation

Panelists:

Tina Gubb
Chief Counsel
FINRA Enforcement

Jordan Materna
Deputy Director, Options Insider Trading Investigations
FINRA Member Supervision

Danny Mileto
Vice President, Options Regulation
FINRA Market Regulation

Steven Price
Senior Vice President, National Cause Program
FINRA Member Supervision

Options Panelists Bios:

Moderator:

Gene DeMaio is Executive Vice President in FINRA's Market Regulation Department where he manages the Options Regulation section and the Trading & Execution examination firm grouping. Prior to joining FINRA, Mr. DeMaio was an Options Market Maker at the American Stock Exchange, and earlier worked as an attorney at the law firm of Kord Lagemann where he represented complainants in securities arbitration disputes. Mr. DeMaio is a graduate of Fordham Law and earned his LL.M at New York University.

Panelists:

Tina Salehi Gubb is Chief Counsel in FINRA's Department of Enforcement. She is responsible for supervising several teams of attorneys who bring enforcement actions on behalf of FINRA and the Exchanges. Her team's disciplinary actions span a broad range of market integrity and investor protection issues, including the Market Access Rule, market manipulation and systemic best execution violations in equity and fixed income markets. In addition, Ms. Gubb has overseen numerous significant enforcement actions involving systemic supervisory deficiencies. Ms. Gubb is a graduate of James Madison University, and the University of Richmond School of Law.

Jordan Materna is Deputy Director in FINRA's National Cause and Financial Crimes Detection Programs for the Options Regulatory Surveillance Authority (ORSA). He has been with FINRA since January 2015 and has been with ORSA since it was formed in 2006. Mr. Materna's area of responsibility includes the direction of Insider Trading surveillance and investigative work that FINRA performs pursuant to the ORSA NMS plan on behalf of all of the U.S. options exchanges. His role also encompasses the coordination of efforts related to equity Insider Trading investigations. Additionally, Mr. Materna works closely with the U.S. Securities and Exchange Commission and has assisted the Federal Bureau of Investigation, the U.S. Attorney's office and foreign regulators, and has provided testimony in federal criminal trial proceedings. Prior to FINRA, Mr. Materna was employed by the CBOE since 1984. He started on the trading floor and worked as an Order Book Official (OBO) before joining the Department of Market Regulation in 1989. Over the next 10 years, Mr. Materna worked in the Regulatory Division as a Senior Investigator, Compliance Examiner and Trading Floor Liaison. In 1999, Jordan was hired to manage the Insider Trading Group and was promoted to Director in 2005 and then Department Head in 2012. Mr. Materna received his B.A. in Business from Western Illinois University.

Danny Mileto is Vice President, Option Regulation within FINRA Market Regulation is responsible for surveillance and investigations of option participants for compliance issues such as Regulation SHO, fraud, manipulation, and various other exchange specific rules. The VP works closely with various teams within FINRA, including Technology and SRM&G, to develop and improve surveillance reports to identify improper activity across exchanges and products. In addition, the VP works proactively with external groups including the SEC, ISG and the various option exchanges. Mr. Mileto has been with FINRA since 2000 and prior to that was an options market maker and specialist with Susquehanna Investment Group. Under his management, the unit worked closely with Enforcement to produce seminal cases involving Regulation SHO and cross product manipulation involving option participants. Mr. Mileto holds a BBA with a concentration in Finance from Iona College. He is also a graduate of FINRA's Leadership at Wharton program.

Steven Price is Senior Vice President and oversees FINRA's National Cause Program, which conducts assessments and investigations of financial industry participants across the U.S. based on triggering events and regulatory intelligence. He also participates in multiple organizational committees and initiatives designed to establish FINRA as a leader in regulatory vision and to advance the protection of investors. Mr. Price re-joined FINRA in 2020 after spending the previous 12 years in multiple roles overseeing broker-dealer compliance and operations for ALPS Distributors and ALPS Portfolio Solutions Distributor. He formerly served in the enforcement units of FINRA and the Colorado Division of Securities, as well as serving on the Colorado Securities Board. Prior to his regulatory roles, Mr. Price was a market maker at the Chicago Board Options Exchange and a litigator with concentration across civil and criminal matters.

Options

Panelists

- **Moderator**
  - Gene DeMaio, Executive Vice President, Options Regulation and T&E, FINRA Market Regulation
- **Panelists**
  - Tina Gubb, Chief Counsel, FINRA Enforcement
  - Jordan Materna, Deputy Director, Options Insider Trading Investigations, FINRA Member Supervision
  - Danny Mileto, Vice President, Options Regulation, FINRA Market Regulation
  - Steven Price, Senior Vice President, National Cause Program, FINRA Member Supervision

To Access Polling

- **Please get your devices out:**
  - Type the polling address, **https://finra.cnf.io/sessions/fg5p** into the browser or scan the QR code with your camera.

  - Select your polling answers.

Polling Question 1

1. **Which of the following regulatory issues impacting options markets are you most interested in hearing about today?**
   a. Consolidated Audit Trail (CAT) data and its benefits
   b. Options as a Complex Product
   c. Options Insider Trading
   d. Options Intrusions

Polling address: **https://finra.cnf.io/sessions/fg5p**

Polling Question 2

2. **When you raise a compliance issue with FINRA, how would you rate the communications?**
   a. Excellent
   b. Good
   c. Needs improvement

Polling address: **https://finra.cnf.io/sessions/fg5p**

Polling Question 3

3. **How familiar are you with CAT data and how FINRA is using CAT to develop better options surveillance reports?**
   a. Very
   b. Somewhat
   c. Not at all

Polling address: **https://finra.cnf.io/sessions/fg5p**

Polling Question 4

4. **How familiar are you with the various ways in which someone can affect an account intrusion in a customer account using options?**
   a. Very
   b. Somewhat
   c. Not at all

Polling address: **https://finra.cnf.io/sessions/fg5p**

Options
Tuesday, May 17, 2022
8:30 a.m. – 9:30 a.m.

Resources:

- FINRA *Information Notice – 2/3/21, Exercise Cut-Off Time for Expiring Options* (February 2021)

  www.finra.org/rules-guidance/notices/information-notice-020321

- FINRA *Regulatory Notice 22-08, FINRA Reminds Members of Their Sales Practice Obligations for Complex Products and Options and Solicits Comment on Effective Practices and Rule Enhancements* (March 2022)

  www.finra.org/rules-guidance/notices/22-08

- FINRA *Regulatory Notice 21-23, FINRA Reminds Member Firms of Requirements Concerning Best Execution and Payment for Order Flow* (June 2021)

  www.finra.org/rules-guidance/notices/21-23

- FINRA *Regulatory Notice 20-32, FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud* (September 2020)

  www.finra.org/rules-guidance/notices/20-32

- FINRA *Regulatory Notice 20-13, FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic* (May 2020)

  www.finra.org/rules-guidance/notices/20-13

- FINRA *Regulatory Notice 15-46, Guidance on Best Execution Obligations in Equity, Options and Fixed Income Markets* (November 2015)

  www.finra.org/rules-guidance/notices/15-46

Information Notice

March 2022 Options Disclosure Document

FINRA is advising member firms that the Options Clearing Corporation has issued the March 2022 Options Disclosure Document (ODD). The ODD contains general disclosures on the characteristics and risks of trading standardized options. The March 2022 ODD: (i) contains supplemental material to accommodate trading of certain index options and index flex options with a multiplier of one; and (ii) makes certain administrative changes to correct references to chapter subtitles contained in the original ODD text and to update references to sections in the document.

Rule 9b-1 under the Securities Exchange Act requires broker-dealers to deliver the ODD and supplements to customers. FINRA has similar requirements in FINRA Rule 2360(b)(11)(A)(1), which, among other things, requires firms to deliver the current ODD to each customer at or before the time the customer is approved to trade options.

To comply with the requirements of FINRA Rule 2360(b)(11)(A)(1), firms may distribute the March 2022 ODD in various ways, including, but not limited to, one of the following:

1. conducting a mass mailing of the March 2022 ODD to all of its customers approved to trade options and who have already received the ODD; or
2. distributing the March 2022 ODD to a customer who has already received the ODD, not later than the time a customer receives a confirmation of a transaction in the category of options to which the amendment pertains.

FINRA reminds firms that they may electronically transmit documents, including the ODD, that they are required to furnish to customers under FINRA rules, provided the firm adheres to the standards contained in the October 1995 and May 1996 Securities and Exchange Commission releases, and as discussed in *Notice to Members 98-03*. Firms may also transmit the ODD to customers who have consented to electronic delivery through the use of a hyperlink.

Questions regarding this *Notice* may be directed to Office of General Counsel at (202) 728-8071.

May 6, 2022

Suggested Routing

- Compliance
- Institutional
- Legal
- Options
- Senior Management
- Trading

Key Topics

- Index Options
- Options
- Options Disclosure Document (ODD)

Referenced Rules & Notices

- FINRA Rule 2360
- Notice to Members 98-03

Conflicts of Interest in Capital Markets and Investment Banking
Tuesday, May 17, 2022
8:30 a.m. – 9:30 a.m.

Join FINRA staff and industry professionals as they discuss helpful tips and tools for managing conflicts of interest in capital markets and investment banking firms. Panelists discuss practices that raise conflict of interest concerns and how to remedy these issues.

Moderator:
Thomas Mellett
Vice President, Capital Markets Firm Examinations
FINRA Member Supervision

Panelists:
Cathleen Mack
Chief Compliance Officer
Solomon Partners

Kathryn Travers
Director, Capital Market Risk Monitoring
FINRA Member Supervision

Osamu Watanabe
General Counsel
Moelis & Company

Conflicts of Interest in Capital Markets and Investment Banking Panelists Bios:

Moderator:

Thomas Mellett is Head of Capital Markets Examinations for FINRA's Member Supervision department. He is responsible for examinations of FINRA members that are primarily engaged in Capital Markets business activities, including Institutional Private Placements, Investment Banking, Mergers & Acquisitions, Product Origination & Wholesaling, and Public Finance, among others. Prior to this role, Mr. Mellett was the District Director of FINRA's San Francisco District Office, where he was responsible for the office's examination and risk monitoring programs. From 2013 to 2015, Mr. Mellett was a Surveillance Director during which time he supervised regulatory coordinators who planed examinations and conducted risk monitoring of member firms. From 2010 through 2012, Mr. Mellett was an Examination Manager responsible for supervising routine examinations of member firms. He transitioned into management after working as an examiner. Mr. Mellett is designated as a Certified Regulatory and Compliance Professional™ (CRCP™) through the FINRA Institute. Mr. Mellett holds a bachelor's degree in finance from Bentley University.

Panelists:

Cathleen Mack, CAMS, is Chief Compliance Officer and AMLCO for Solomon Partners Securities, LLC, an investment bank and registered broker-dealer focused on financial advisory services. Prior to joining Solomon Partners in June 2019, Ms. Mack spent 15 years at UBS Investment Bank leading the Conflict Clearance Unit and 5 years at Merrill Lynch in various roles. Ms. Mack is responsible for the oversight of all aspects of the firm's compliance program including but not limited to regulatory matters, employee compliance, outside business interests, conflicts of interest, and AML policies and procedures. Ms. Mack is CAMS certified and a member of the Association of Certified Anti-Money Laundering Specialists. She graduated from Seton Hall University with a B.S. in Physics and holds FINRA 7, 63, 4, and 24 licenses.

Kathryn Travers is Risk Monitoring Director in the M&A Investment Banking in FINRA's Boston Office. Ms. Travers has more than 20 years of experience in the investment industry with 17 of those employed by FINRA. Her responsibilities include managing the Risk Monitoring Analysts in her section that are responsible for monitoring the financial and sales practice day-to-day activities of 250 member firms. Ms. Travers is a graduate of Stonehill College with a double major in Economics and Political Science. She also obtained her Certified Fraud Examiner (CFE) designation in 2016.

Osamu Watanabe is the General Counsel of Moelis & Company, a leading independent investment bank listed on the NYSE. Mr. Watanabe joined Moelis & Company as a newly founded investment bank and managed its successful IPO. Mr. Watanabe was also General Counsel for Moelis Asset Management which includes MCP private equity funds, Gracie credit hedge funds, Freeport direct lending funds and Steele Creek CLO funds. Prior to joining Moelis & Company, Mr. Watanabe held senior positions at Sagent Advisors, UBS, Credit Suisse First Boston and Donaldson, Lufkin & Jenrette. Mr. Watanabe was in private practice at Sullivan & Cromwell in New York, Tokyo, Hong Kong and Melbourne for 10 years focusing on U.S. and international securities offerings, M&A transactions, restructurings, bank financings, real estate transactions, and broker-dealer, bank and investment company regulation. Mr. Watanabe clerked for the Honorable Morey L. Sear, Eastern District of Louisiana. Mr. Watanabe holds a B.A. from Antioch College (1982) and a J.D. from Yale Law School (1985).

Conflicts of Interest in Capital Markets and Investment Banking

Panelists

- **Moderator**
  - Thomas Mellett, Vice President, Capital Markets Firm Examinations, FINRA Member Supervision
- **Panelists**
  - Cathleen Mack, Chief Compliance Officer, Solomon Partners
  - Kathryn Travers, Director, Capital Market Risk Monitoring, FINRA Member Supervision
  - Osamu Watanabe, General Counsel, Moelis & Company

Scenario: Two Teams, Two Engagements

- A firm has two Advisory Teams, Team “Wall Street” and Team “Sandhill Road”.
- Team Wall Street engaged in detailed buy-side talks with client “Really Smart Fund” about purchasing company “Next Big Thing”. Team Wall Street was provided with the bid range Really Smart Fund is willing to pay for Next Big Thing. Due to an operational breakdown, Team Wall Street did not timely initiate the firm’s conflict clearing process.
- Team Sandhill Road entered sell-side talks with client Next Big Thing. Team Sandhill Road submitted its engagement with Next Big Thing to the firm’s conflict clearance process and the engagement was cleared.
- Team Wall Street discovers its operational oversight and submits the engagement with Really Smart Fund to the firm’s conflict clearing process late.

Conflicts of Interest in Capital Markets and Investment Banking
Tuesday, May 17, 2022
8:30 a.m. – 9:30 a.m.

Resources:

- FINRA's Conflicts of Interest Webpage

  www.finra.org/rules-guidance/key-topics/conflicts-of-interest

- FINRA Report on Conflicts of Interest (October 2013)

  www.finra.org/sites/default/files/Industry/p359971.pdf

Challenges Facing Firms in Monitoring AML and Protecting Against Fraudulent Activities

Tuesday, May 17, 2022
9:45 a.m. – 10:45 a.m.

This session reviews challenges facing firms in monitoring and protecting against fraudulent activities. Join FINRA staff and industry panelists as they provide examples of effective controls their firms have put into place to address AML risks.

Moderator:

Gargi Sharma
Director, Special Investigation Unit
FINRA Member Supervision

Panelists:

Chris Covington
Assistant Special Agent in Charge - Pandemic Response Accountability Committee (PRAC)
Council of the Inspectors General on Integrity and Efficiency (CIGIE)

Sarah Green
Global Head of Financial Crimes
The Vanguard Group Inc.

Kara Williams
Senior Principal Investigator, Special Investigation Unit
FINRA Member Supervision

Challenges Facing Firms in Monitoring AML and Protecting Against Fraudulent Activities
Panelists Bios:

Moderator:

Gargi Sharma is Investigative Director within FINRA's Special Investigation Unit and supports a team of five investigators who conduct complex Anti-Money Laundering and Fraud investigations. Ms. Sharma is also involved with identifying industry trends that pose compliance risk, especially related to Anti-Money Laundering, and providing training internally within FINRA and to the industry. Ms. Sharma is a Certified Anti-Money Laundering Specialist and graduated from the University of Texas with bachelor's and master's degrees in Finance and Accounting. Ms. Sharma works from FINRA's Florida Office and has been with FINRA for 13 years.

Panelists:

Chris Covington is the Joint Operations Manager at the Pandemic Response Accountability Committee (PRAC). He joined the PRAC in April 2021 after a brief stint at the Healthcare Fraud Prevention Partnership. Mr. Covington manages the PRAC Fraud Task Force which has 41 agents from 12 Offices of Inspector General. The task force is focused on Pandemic loan fraud involving the Paycheck Protection Program and Economic Injury Disaster Loan program. Mr. Covington retired from the U.S. Department of Health and Human Services Office of Inspector General in September 2020. During his 21-year career, he served as both a Special Agent and Assistant Special Agent in Charge. Mr. Covington is Phi Beta Kappa graduate of the University of Tennessee and holds a master's degree in political science from Vanderbilt University.

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

Kara Williams is Senior Principal Investigator in the Special Investigation Unit at FINRA, where she conducts complex AML and Fraud investigations. In addition to her regulatory experience, Ms. Williams is also actively involved with FINRA's Advanced Analytics Program. During her 8 years at FINRA, Ms. Williams has served in various investigative roles identifying high risk activity within Member Supervision and the National Cause and Financial Crimes Detection Programs.

Challenges Facing Firms in Monitoring AML and Protecting Against Fraudulent Activities

Panelists

- **Moderator**
  - Gargi Sharma, Director, Special Investigation Unit, FINRA Member Supervision
- **Panelists**
  - Chris Covington, Assistant Special Agent in Charge - Pandemic Response Accountability Committee (PRAC), Council of the Inspectors General on Integrity and Efficiency (CIGIE)
  - Sarah Green, Global Head of Financial Crimes, The Vanguard Group Inc.
  - Kara Williams, Senior Principal Investigator, Special Investigation Unit, FINRA Member Supervision

To Access Polling

- **Please get your devices out:**
  - Type the polling address, **https://finra.cnf.io/sessions/saj2** into the browser or scan the QR code with your camera.

  - Select your polling answers.

Polling Question 1

1. **Have you read the relevant sections of the FINRA's Report on Examination and Risk Monitoring and SEC Examination Priorities?**
   a. Yes
   b. No
   c. What are these?

Polling address: **https://finra.cnf.io/sessions/saj2**

Polling Question 2

2. **How informed are you on different types of Cyber-Enabled Financial Crimes, and related red flags and effective practices?**
   a. Very informed
   b. Somewhat informed
   c. Not informed at all
   d. Does not apply to my firm

Polling address: **https://finra.cnf.io/sessions/saj2**

Polling Question 3

3. **How has your firm staying abreast of the recent sanctions?**
   a. Treasury/OFAC website
   b. FinCEN Advisories
   c. FINRA Notices
   d. All or some of the above
   e. Does not apply to my firm

Polling address: **https://finra.cnf.io/sessions/saj2**

Challenges Facing Firms in Monitoring AML and Protecting Against Fraudulent Activities

Tuesday, May 17, 2022
9:45 a.m. – 10:45 a.m.

Resources:

FinCEN's Resources:

- FinCEN's, *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime* (October 2016)

  www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf

- FinCEN's, Frequently Asked Questions (FAQs) regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through Suspicious Activity Reports (SARs) (October 2016)

  www.fincen.gov/frequently-asked-questions-faqs-regarding-reporting-cyber-events-cyber-enabled-crime-and-cyber

- FinCEN's, *Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic* (July 2020)

  www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cybercrime%20508%20FINAL.pdf

- FinCEN's, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments* (October 2020)

  www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf

- FinCEN's AML and Countering the Financing of Terrorism National Priorities and Statement – June 2021

  www.fincen.gov/news/news-releases/fincen-issues-first-national-amlcft-priorities-and-accompanying-statements

  www.fincen.gov/sites/default/files/shared/Statement%20for%20Non-Bank%20Financial%20Institutions%20(June%2030%2C%202021).pdf

FINRA Resources:

- FINRA *Regulatory Notice 22-06, U.S. Imposes Sanctions on Russian Entities and Individuals* (February 2022)

  www.finra.org/rules-guidance/notices/22-06

- FINRA *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* (October 2021)

  www.finra.org/rules-guidance/notices/21-36

- FINRA *Regulatory Notice 21-18, FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts* (May 2021)

  www.finra.org/rules-guidance/notices/21-18

- FINRA *Regulatory Notice 21-14, FINRA Alerts Firms to Recent Increase in ACH "Instant Funds" Abuse* (March 2021)

  www.finra.org/rules-guidance/notices/21-14

- FINRA *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* (February 2021)

  www.finra.org/rules-guidance/notices/21-03

- FINRA *Regulatory Notice 20-32, FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection with Potential Account Takeovers and New Account Fraud* (September 2020)

  www.finra.org/rules-guidance/notices/20-32

- FINRA *Regulatory Notice 20-13, FINRA Reminds Firms to Beware of Fraud During the COVID-19 Pandemic)* (May 2020)

  www.finra.org/rules-guidance/notices/20-13

- FINRA *Regulatory Notice 19-18, FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligation* (May 2019)

  www.finra.org/rules-guidance/notices/19-18

- FINRA Unscripted Podcast - Overlapping Risks, Part 1: Anti-Money Laundering and Cybersecurity

  www.finra.org/media-center/finra-unscripted/aml-cybersecurity

- FINRA Unscripted Podcast - At, By or Through: Fraud in the Broker-Dealer Industry

  www.finra.org/media-center/finra-unscripted/fraud-broker-dealer-industry

- FBI Cyber Threat Briefing Series

  www.finra.org/events-training/conferences-events/fbi-cyber-threat-briefing-series

- *2022 Report on FINRA's Examination and Risk Monitoring Program* (February 2022)

  www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program

- FINRA Firm Checklist for Compromised Accounts

  www.finra.org/rules-guidance/key-topics/customer-information-protection/firm-checklist-compromised-accounts

- FINRA Firm Identity Protection

  www.finra.org/rules-guidance/guidance/firm-identity-protection

- FINRA's Sanctions Alert: Russia-Related Sanctions

  www.finra.org/rules-guidance/key-topics/aml/sanctions-alert-russia-related-sanctions-022822

- SEC Regulation S-ID – Includes Identify Theft Red Flags Rule Template

  www.finra.org/rules-guidance/key-topics/customer-information-protection/ftc-red-flags-rule

Other Resources:

- U.S. Department of the Treasury Press Release, *Treasury Publishes National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing* (March 2022)

  www.home.treasury.gov/news/press-releases/jy0619

- U.S. Department of the Treasury, OFAC's Information Hub for Ukraine-Russia Related Sanctions

  www.home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions

- SEC *Risk Alert: Compliance Issues related to Suspicious Activity Monitoring and Reporting* (March 2021)

  www.sec.gov/files/aml-risk-alert.pdf

- SEC *Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities*

  www.sec.gov/tm/risks-omnibus-accounts-transacting-low-priced-securities

- FBI Internet Crime Complaint Center IC3

  www.ic3.gov/Home/ComplaintChoice/default.aspx

- The Federal Reserve - Synthetic Identity Fraud Mitigation Toolkit

  www.fedpaymentsimprovement.org/synthetic-identity-fraud-mitigation-toolkit/?utm_campaign=20220405_NFS_PR_IRP_SIF%20Toolkit%20Phase%202.1_FPI%20Community&utm_medium=email&utm_source=Eloqua

Emails

- Common nomenclature
- Email dotting
- Questionable domains

We have chosen Switzerland as our home because we believe it provides strong legal privacy protections.

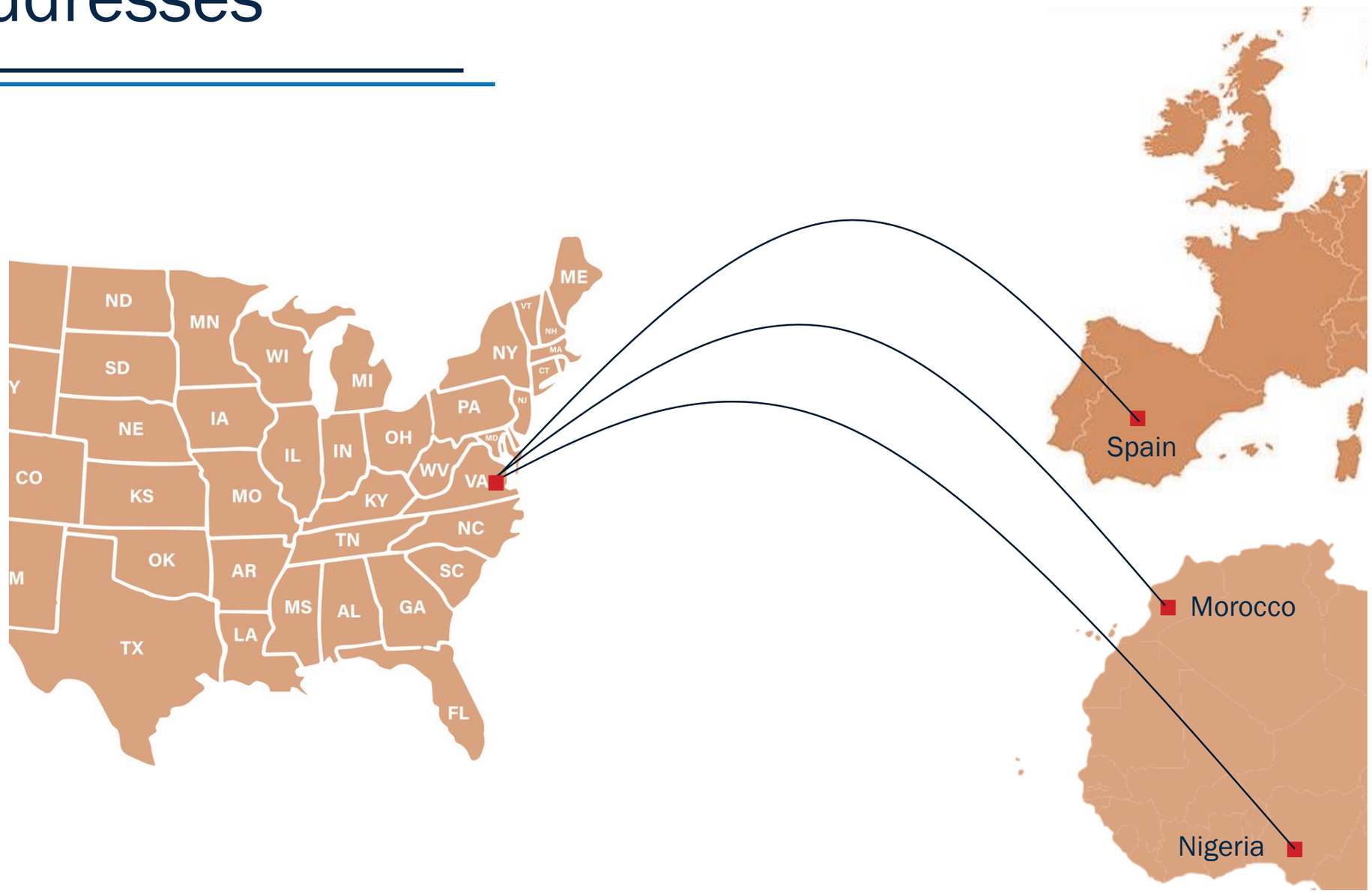
Top 6 Disposable Email Address Services

Use a disposable email address to eliminate spam from your inbox

Virtual Mailbox Services

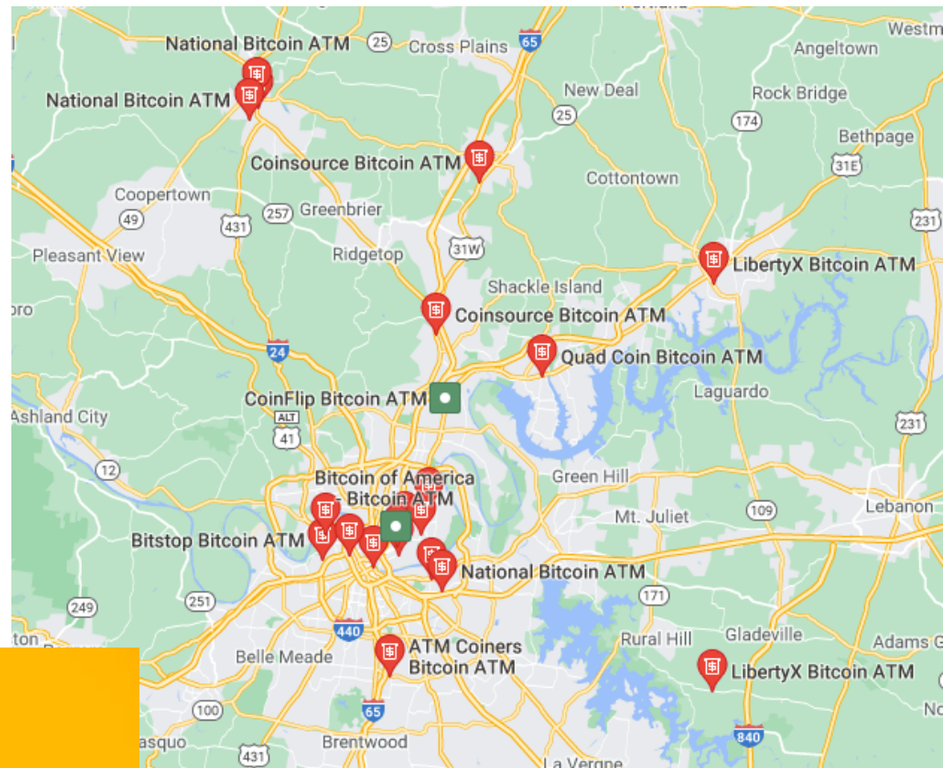
PhysicalAddress.com

IP Addresses



Cryptocurrency

- There are over 25,142 crypto ATMs in the United States
  - Canada: 2,267
  - European Union: 1,396



2022 Annual Conference

May 16 –18 | Washington, DC | Hybrid Event

Communications Compliance: Current Developments

Tuesday, May 17, 2022
9:45 a.m. – 10:45 a.m.

Join FINRA staff and industry panelists for a discussion of current communications compliance and marketing practices. Topics include recent guidance on how FINRA's communications rules apply in a virtual environment, and how firms can communicate compliantly about ESG and other current investment trends. Panelists also talk about the regulatory implications of complex products and services such as crypto assets and emerging technologies in the marketing compliance space.

Moderator:

Ira Gluck
Director
FINRA Advertising Regulation

Panelists:

Suzanne Bond
Senior Vice President and Chief Compliance Officer
Inland Securities Corporation

Pramit Das
Director
FINRA Advertising Regulation

Sheelagh Howett
Chief Risk Officer and Chief Compliance Officer
Cantella & Co., Inc.

Communications Compliance: Current Developments Panelists Bios:

Moderator:

Ira Gluck is Director in FINRA's Advertising Regulation Department. In this role, he works on rulemaking and policy issues and is responsible for the Department's complex review and spot-check programs. Mr. Gluck's previous positions within FINRA included leading the Emerging Regulatory Issues team as well as heading the Strategic Initiatives Group in FINRA's Enforcement Department. He also served in various investigative and management roles in the Enforcement and Member Regulation Departments of NASD before its 2007 consolidation with NYSE Member Regulation, which resulted in the formation of FINRA. Mr. Gluck received his bachelor's degree from the University of Pennsylvania and completed both a master's degree and M.B.A. at the University of California, Irvine.

Panelists:

Suzanne L. Bond is a highly regarded Chief Compliance Officer with a demonstrated track record for over 25 years in various sectors of the financial services industry. She began her career with a national wire house in fixed income and futures, and further expanded her expertise across regional and independent broker/dealers, and registered investment advisory firms where she has held positions in sales, marketing and compliance. In her current role as Senior Vice President, Chief Compliance Officer of Inland Securities Corporation, the affiliated dealer/manager of Inland Real Estate Investment Corporation, Ms. Bond contributes her skills in areas of business governance and risk management, investment management practices, alternative investment markets, and compliance management. She is a strong influencer to senior business stakeholders, assisting with strategic planning, operational procedure, employee compensation, and technology systems development. Prior to joining Inland, Ms. Bond served as Vice President and Director of Supervision for the Capital Markets Group at Wedbush Securities. Prior to that, she served as Chief Compliance Officer for a number of independent broker/dealers and investment advisory firms, both retail and institutional. In January 2020, Ms. Bond was appointed to the Financial Industry Regulatory Authority ("FINRA") Midwest Region Committee for a three-year term. She is a frequent panelist/guest speaker at national industry events including the inaugural SEC Compliance Outreach Program. Ms. Bond holds a B.S. in International Business from Union Institute & University and a Master of Jurisprudence, Business Law from Loyola University Chicago. She is fluent and/or conversant in six languages, and holds FINRA Series 7, 24, 63, 66, 79, and 99 licenses.

Pramit Das is Director in FINRA's Advertising Regulation Department. In this role, his responsibilities include managing the Department's filings review program, operations, administration and, proprietary technology systems. He also provides education to members, FINRA staff and other regulatory staff and, participates in rule amendment and rulemaking projects as necessary. Prior to joining FINRA (fka NASD) in 1994, Mr. Das worked for Metropolitan Life Insurance Company and Arthur Andersen & Co. He holds an MBA in Finance from the University of Maryland, College Park, and an MA in Financial Economics from Clemson University, Clemson, South Carolina. He was also Series 7 and 63 registered.

Sheelagh Howett is Chief Risk Officer and Chief Compliance Officer at Cantella & Co., Inc. She is on the Board of Directors and shares leadership responsibility with the executive management team for overseeing the growth and success of the firm. She focuses on keeping clear and regular communication between business units and compliance within the firm. She strongly believes that risk is an enterprise-wide responsibility and has created a risk-aware culture including an understanding that risk prevention is everyone's job. She continually works to further develop risk-management processes to identify, assess, and respond to the inevitable risks that face our industry. At the same time, she works to improve the efficiency and integration of existing processes into daily routines, so they become ingrained in the firm's business. Ms.

Howett is a member of the New England Broker/Dealer Investment Advisor Association, and the Women in Pensions Network. Originally from Ireland, Ms. Howett earned a BA in Banking and Finance at University College in Dublin. She holds FINRA Series 7 and 24 licenses.

Communications Compliance: Current Developments

Panelists

- **Moderator**
  - Ira Gluck, Director, FINRA Advertising Regulation
- **Panelists**
  - Suzanne Bond, Senior Vice President and Chief Compliance Officer, Inland Securities Corporation
  - Pramit Das, Director, FINRA Advertising Regulation
  - Sheelagh Howett, Chief Risk Officer and Chief Compliance Officer, Cantella & Co., Inc.

Agenda

- Compliance in a Virtual Environment
- Current Issues
- Emerging Technologies and Digital Communications
- Questions
- Wrap-up

01 | Compliance in a Virtual Environment

Compliance in a Virtual Environment

- Compliance Program Changes
- Hybrid Work Environments
- FINRA FAQ

02 | Current Issues

Current Issues

- Crypto Assets
- Complex Products
- ESG

03 | Emerging Technologies and Digital Communications

Emerging Technologies and Digital Communications

- New Digital Platforms
- Video
- Firm Approaches to Digital Communications
- FINRA Observations
- Working with FINRA Staff
- Emerging Concerns

04 | Questions

05 | Wrap-up

Frequently Asked Questions About Advertising Regulation

On This Page

FINRA Rule 2210 Interpretive Guidance

A. Definitions

A.1. Institutional Communications

A.1.1. Q. If a firm distributes an institutional communication to intermediaries that fall within the definition of "institutional investor" and labels the communication for use only with institutional investors, and an intermediary subsequently distributes the communication to retail investors, is the member then required to treat the communication as a retail communication?

A. Unless the firm becomes aware that the intermediary has distributed the communication to retail investors, or the firm has not adequately labeled the communication, the firm will not be required to treat the communication as retail. FINRA Rule 2210(a)(3) defines "institutional communication" as "any written (including electronic) communication that is distributed or made available only to institutional investors, but does not include a member's internal communications." FINRA Rule 2210(a)(4) (the definition of "institutional investor") states in part that "No member may treat a communication as having been distributed to an institutional investor if the member has reason to believe that the communication or any excerpt thereof will be forwarded or made available to any retail investor."

For example, a broker-dealer that receives an institutional communication from a mutual fund underwriter is responsible for assuring that its associated persons do not forward the communication to retail investors. The "reason to believe" standard is not intended to require a mutual fund underwriter to audit recipient broker-dealers' use of institutional communications.

Assuming a firm adequately labels an institutional communication as being for institutional use only, the firm would not have reason to believe, absent other facts, that the communication will be distributed to retail investors. However, if the recipient broker-dealer informs the fund underwriter that it intends to distribute the communication to its retail customers, or the fund underwriter otherwise becomes aware of this practice, the fund underwriter must either treat the communication as a retail communication going forward, or cease distributing institutional communications to the recipient broker-dealer until it reasonably concludes that the broker-dealer has adopted appropriate procedures to prevent redistribution.

Posted: 5/22/15

A.1.2. Q. FINRA Rule 2210(a)(3) defines "institutional communication" to exclude a firm's internal communications. Does "internal communication" include training and educational material prepared for use with registered representatives of affiliated broker-dealers?

A. No. "Internal communication" refers to communications within a firm. If a firm uses material to train or educate registered representatives of other broker-dealers (whether affiliated or unaffiliated), the material would be considered an institutional communication.

Posted: 1/7/13

B. Principal Approval

B.1. Third Party Research Reports

B.1.1. Q. If a firm distributes only to institutional investors a third-party research report that does not qualify as an independent third-party research report pursuant to FINRA Rule 2241(a)(3), is the firm required to have a registered principal or supervisory analyst approve the report prior to distribution?

A. No. A third-party research report that is distributed only to institutional investors as defined in FINRA Rule 2210(a)(4) is considered an institutional communication under FINRA Rule 2210(a)(3). FINRA Rule 2210(b)(3) permits a firm to distribute an institutional communication without having a registered principal approve the communication prior to distribution, provided that the firm establishes and implements certain written procedures for the supervision and review of such communications.

FINRA Rule 2241(h)(1) requires a registered principal or supervisory analyst to review for compliance with the applicable provisions of Rule 2241(h) and approve third-party research reports distributed by the firm unless the report meets the definition of "independent third-party research report."[1] However, this rule is not intended to require registered principal or supervisory analyst approval of a third-party research report that meets the definition of institutional communication. Accordingly, a firm may supervise such a report in the same manner as any other institutional communication pursuant to FINRA Rule 2210(b)(3).[2]

Updated: 12/14/15

B.2. Business Development Companies

B.2.1. Q. Does a Series 26 registration (Limited Principal - Investment Company and Variable Contracts Products) qualify a principal to approve a retail communication concerning a BDC?

A. No. A BDC is not registered as an investment company under the Investment Company Act of 1940. Accordingly, the Series 26 registration does not qualify a principal to approve a retail communication concerning a BDC. To approve a retail communication concerning a BDC, the registered principal must possess either a Series 24 (General Securities Principal), a Series 9/10 (General Securities Sales Supervisor) or a Series 39 (Limited Principal - Direct Participation Programs) registration, if the BDC is structured as a direct participation program as defined in NASD Rule 1022(e)(2).[3]

Posted: 5/22/15

B.3. Questions concerning principal approval of non-promotional communications (see Section C.4.) and for social media posts in online interactive electronic forums (see section C.6.).

C. Filing Requirements and Filing Exclusions

C.1. Filing Requirements

C.1.1. Q. Is a firm required to file with FINRA a retail communication concerning a business development company (BDC) that is registered under the Securities Act?

A. Yes. BDCs fall within the definition of direct participation program under FINRA Rule 2310(a)(4). Accordingly, firms must file with FINRA retail communications concerning BDCs that are registered under the Securities Act within 10 business days of first use or publication pursuant to FINRA Rule 2210(c)(3)(B).

Posted: 5/22/15

C.1.2. Q. FINRA Rule 2210(c)(3)(E) requires a firm to file within 10 business days of first use or publication retail communications concerning any security that is registered under the Securities Act of 1933 and that is derived from or based on a single security, a basket of securities, an index, a commodity, a debt issuance or a foreign currency (registered structured products). What types of products does this filing requirement cover?

A. While it is not possible to list all registered structured products, examples include exchange-traded notes that are not registered under the Investment Company Act but are registered under the Securities Act, registered reverse convertibles, registered structured notes, registered principal protection notes, and any other registered security that includes embedded derivative-like features. See Regulatory Notice 12-03 for some examples of registered structured products.

The purpose of this filing requirement is to have firms file with FINRA retail communications about structured products that are registered under the Securities Act. It is not intended to create a duplicative requirement for retail communications that are already subject to filing, such as retail communications concerning mutual funds, closed-end funds, exchange-traded funds that are registered under the Investment Company Act, variable insurance products, direct participation programs or collateralized mortgage obligations.

While this filing requirement applies to retail communications concerning registered structured products, it does not apply to issuer-prepared prospectuses, including issuer-prepared free-writing prospectuses that are filed with the SEC.[4]

Posted: 1/7/13

C.2. Filing Exclusion for Non-Material Changes to Previously Filed Retail Communications

C.2.1. Q. If a firm has previously filed a retail communication and then decides to use the same communication in a different format, must the firm refile the communication as it appears in the new format?

A. No. FINRA Rule 2210(c)(7)(A) excludes from filing retail communications that previously have been filed with FINRA and that are used without material change. FINRA would not consider revising a retail communication to appear in a different format to be a material change, provided that the content has not materially changed. For example, if a firm has previously filed a retail communication in the format that it appears on a desktop or laptop computer, and the firm is redesigning the presentation to appear on a tablet or smart phone, the firm would not have to refile the version that will appear on a tablet or smart phone.

Posted: 5/22/15

C.2.2. Q. What if a firm uses responsive Web design technology[5] to deliver a retail communication in different formats depending on the device used by a customer? Must the firm file each version of the retail communication to show how it will appear on each device?

A. No. For the same reasons set forth in the answer to the previous question, FINRA would not consider delivery of the same content in a retail communication in different formats using responsive design technology to be a material change to the communication. Accordingly, a firm would only have to file the retail communication once.

Posted: 5/22/15

C.2.3. Q. If a firm previously filed a retail communication that was initially distributed in print form, and the firm later decides to post the same communication on its website, must the firm refile the website version of the retail communication with FINRA?

A. No, provided that the content of the website version of the retail communication appears without material change from the previously filed print version.

Posted: 5/22/15

C.2.4. Q. If a firm changes the color scheme of a previously filed retail communication, must the firm refile the new version of the retail communication?

A. No. FINRA would not regard merely changing the color scheme of a previously filed retail communication to be a material change to the communication.

Posted: 5/22/15

C.2.5. Q. Is a firm required to re-file retail communications concerning a mutual fund that changes its name, if the only changes to the previously filed communications are substitutions of the fund's new name for its old name?

A. No. Assuming the fund has changed its name in any required filings with the SEC, FINRA would not consider merely changing the fund's name from previously filed retail communications concerning the fund to be a material change to the communications.

Posted: 5/22/15

C.2.6. Q. If a mutual fund passes its five-year or ten-year anniversary since inception, and a firm adds a new line to previously filed retail communications that present fund performance to show the fund's five-year or ten-year performance record as required by SEC Rule 482, must the firm re-file the revised retail communications?

A. No. FINRA would not consider merely adding a fund's five-year or ten-year performance record as required by Rule 482 to previously filed retail communications to be a material change.

Posted: 5/22/15

C.2.7 Q. The SEC presumes that the use of the terms “adviser” or “advisor” in a name or title by a broker-dealer that is not also registered as an investment adviser, or an associated person that is not also a supervised person of an investment adviser, to be a violation of the capacity disclosure requirement under Regulation Best Interest. If a firm previously filed a retail communication with FINRA, but now needs to revise the communication to eliminate references to adviser or advisor in the firm’s name or an associated person’s title because of Regulation Best Interest’s presumption, would the firm be required to re-file the communication with FINRA?

A. No. Provided that the only revisions to the previously filed retail communication are eliminating references to adviser or advisor in order to comply with Regulation Best Interest, the firm would not be required to re-file the communication. Under these facts, FINRA would not consider such revisions to be a material change.

Posted: 5/20/20

C.3. Filing Exclusion for Templates

C.3.1. Q. A firm acts as a principal underwriter of a mutual fund family, and each fund in the family offers multiple classes of shares. If the firm creates a separate fact sheet for each share class of every fund in the family, is the firm required to file every fact sheet with FINRA if the only differences between the fact sheets for each share class of a particular fund are a share class's sales load, fees and performance?

A. No. FINRA Rule 2210(c)(7)(B)(i) excludes from filing retail communications that are based on templates that were previously filed with FINRA the changes to which are limited to updates of more recent statistical or other non-narrative information. If a firm files fact sheets for all share classes of one fund in its fund family, and the share class fact sheets for other funds follow the same format in presenting sales load, fee and performance information, then the firm would not be required to file the fact sheet for each share class of the other funds in the family. Instead, pursuant to the filing exclusion for templates, the firm would be permitted to file the fact sheet for only one share class of each of the other funds in the fund family. The firm should indicate as part of its filing that it is relying on the filing exclusion for templates in cases where the firm is filing only one share class fact sheet for a particular fund.[6]

Posted: 5/22/15

C.4. Non-Promotional Communications

C.4.1. Q. Is a firm required to file with FINRA, or have a principal approve prior to use, a retail communication that is limited to market commentary concerning overall changes in the market on a particular day, or a discussion of economic news?

A. No. General market commentaries or economic discussions that are not used for the purpose of promoting a product or service of the firm would be considered retail communications that do not make any financial or investment recommendation or otherwise promote a product or service of the member. See FINRA Rules 2210(b)(1)(D)(iii) and 2210(c)(7)(C).

Posted: 5/22/15

C.4.2. Q. Is a firm required to file, or have a principal approve prior to use, a retail communication that merely explains factual information regarding an individual retirement account, qualified plan or 401(k) account?

A. No. These kinds of retail communications also would be considered to be non-promotional and thus not subject to the principal pre-use approval or filing requirements. See FINRA Rules 2210(b)(1)(D)(iii) and 2210(c)(7)(C).

Posted: 5/22/15

C.4.3. Q. Is a firm required to file, or have a principal approve prior to use, a retail communication that merely provides information to participants in an employee retirement plan as required by the Employee Retirement Income Security Act of 1974 (ERISA) or the current Department of Labor (DOL) rules under ERISA? For example, would a firm be required to file a retail communication that merely informs participants in an employee retirement plan of changes to the investment options that are available through the plan?

A. In most cases, no. A firm would not be required to file or have a principal approve prior to use a notice distributed to plan participants that is required by ERISA or DOL rules, such as a notice that merely informs the participants of investment options that will no longer be available through the plan as of a particular date, and the investment options that will replace the eliminated options.

FINRA would consider such a notice to be a retail communication that does not make any financial or investment recommendation or otherwise promote a product or service of the member. However, if the notice also includes performance or other information that describes the investment objectives of the new investment options, or otherwise includes a headline or other graphic or text that promotes these new options, the firm would be required to file the notice, unless this information is required by ERISA or DOL rules.[7]

Posted: 5/22/15

C.4.4. Q. Is a firm required to file its stationery or the business cards of its associated persons?

A. No. These communications are not subject to filing requirements.

Posted: 5/22/15

C.4.5. Q. Is a firm required to have a principal approve prior to use or file with FINRA a video posted online that does not recommend or promote a product or service of the firm? New

A. No. In accordance with the exceptions in FINRA Rules 2210(b)(1)(D)(iii) and (c)(7)(C), a firm is not required to have a principal approve prior to use or file with FINRA a video posted online that does not recommend or promote a product or service of the firm, provided that the firm supervises and reviews such videos in the same manner as correspondence pursuant to FINRA Rules 3110(b) and 3110.06 through .09.[8] For example, FINRA Rule 3110(b)(4) requires that a firm's written supervisory procedures include procedures for the review of electronic communications related to the firm's investment banking or securities business and such procedures must be appropriate for each firm's business, size, structure, and customers.

Posted: 9/30/21

C.5. Article Reprints

C.5.1. Q. If a firm wishes to distribute to its customers a reprint of an article concerning a product subject to one of the filing requirements that appeared in an unaffiliated magazine or newspaper, and the only change that the firm made to the article was to add the firm's name and any disclosures necessary to meet applicable regulatory standards, is the firm required to file the article reprint with FINRA?

A. No. If a firm merely adds its name to the reprint or adds disclosures required to make the reprint consistent with applicable regulatory standards, the firm is not required to file the reprint with FINRA pursuant to FINRA Rule 2210(c)(7)(I).[9]

Posted: 5/22/15

C.6. Social Media Posts in Online Interactive Electronic Forums

C.6.1. Q. Did the adoption of FINRA Rule 2210 change the exceptions from the principal pre-use approval and filing requirements for posts in the interactive electronic forum portions of social media as compared to the requirements under NASD Rule 2210?

A. No, these exceptions have not changed. NASD Rule 2210 included as a communication category public appearances, which was defined to include participation in an interactive electronic forum. NASD Rule 2210 did not require principals to approve public appearances prior to use, and did not require firms to file public appearances with FINRA.

FINRA Rule 2210 treats interactive electronic forum posts, such as social media status updates, as retail communications rather than public appearances; however, the rule specifically excludes these posts from both the principal pre-use approval requirements and the filing requirements. See FINRA Rules 2210(b)(1)(D)(ii) and 2210(c)(7)(M). Accordingly, these exceptions have not changed with respect to posts on interactive electronic forums, despite the fact that they are no longer considered public appearances for purposes of the rule.[10]

Posted: 5/22/15

D. Content Standards

D.1. Disclosure of Expense Reimbursement Arrangements in Mutual Fund Performance Advertising

D.1.1. Q. If a firm presents mutual fund performance information in a retail communication, and the fund's expenses are subsidized through a fee waiver or expense reimbursement arrangement, must the firm disclose this arrangement?

A. FINRA Rule 2210(d)(5)(A) requires retail communications and correspondence that present non-money market fund open-end management investment company performance data as permitted by Securities Act Rule 482 and Investment Company Act Rule 34b-1 to disclose, among other things, the fund's total annual operating expense ratio, gross of any fee waivers or expense reimbursements, as stated in the fund's prospectus fee table.

FINRA also permits a firm to present in performance communications the fund's subsidized expense ratio, as long as the firm presents both the gross and subsidized expense ratios in a fair and balanced manner. If a firm wishes to present a fund's subsidized expense ratio in correspondence or retail communications, the communication must disclose whether the fee waivers or expense reimbursements were voluntary or mandated by contract, and the time period, if any, during which the fee waiver or expense reimbursement obligation remains in effect.[11]

Posted: 5/22/15

D.1.2. Q. May a retail communication or correspondence concerning a mutual fund also include an "adjusted expense ratio" that illustrates the impact of interest and dividend expenses incurred by the fund from borrowings, repurchase agreements or investments in short sales?

A. Yes. Because interest and dividend expenses incurred from borrowings, repurchase agreements or investments in short sales (whether directly or through investments in underlying funds) are considered fund expenses under generally accepted accounting principles, they must be included in a fund's gross and net expense ratios disclosed in the prospectus fee table. Provided that the communication includes the fund's gross and net expense ratios, it also may include an "adjusted expense ratio" that is the fund's gross expense ratio reduced by any amounts contractually waived or reimbursed, and further reduced by interest and dividend expenses resulting from borrowings, repurchase agreements or investments in short sales. The communication should clearly label, and include a prominent plain English explanation of, the adjusted expense ratio, which should be presented separately from, and with no greater prominence than, the fund's gross and net expense ratios.

Posted: 12/2/19

D.2. Recommendations

D.2.1. Q. Do the disclosure requirements regarding recommendations apply to a mutual fund portfolio manager's discussion of the fund's past performance (such as a manager's discussion that accompanies an annual or semi-annual report)?

A. No. While these discussions must comply with FINRA Rule 2210, FINRA does not consider a portfolio manager's discussion of a fund's past performance to be a firm's recommendation of the individual securities included in the discussion.

Posted: 1/7/13

D.3. Provision of Related Performance Information

D.3.1. Q. FINRA's letter to Edward P. Macdonald, Hartford Funds Distributors, LLC ("Hartford"), dated May 12, 2015 ("Hartford Letter") interpreted FINRA Rule 2210 to allow Hartford to include Related Performance Information in communications concerning mutual funds that are distributed solely to institutional investors, as that term is defined in FINRA Rule 2210(a)(4), subject to enumerated representations and conditions. Provided that the presentation is consistent with the representations and conditions contained in the Hartford Letter, may a firm show Related Performance Information that is net of the fees and expenses of the advertised mutual fund?

A. Yes. In condition 5 of the Hartford Letter, Hartford represented that the presentation of Related Performance[12] Information will disclose performance information that is net of fees and expenses of Related Accounts[13], or net of a model fee that is the highest fee charged to any account managed in the strategy. Condition 5 also stated that the fees and expenses of the registered fund that is the subject of the institutional communication will be prominently disclosed and this fund's performance will reflect all fees and expenses. Condition 5 also stated that if the registered fund's fees and expenses are higher than the Related Accounts' fees and expenses, that fact will be disclosed.

A presentation of Related Performance Information that is net of all fees and expenses of the registered mutual fund that is the subject of an institutional communication, rather than the fees and expenses of the Related Accounts, is consistent with the intent of the Hartford Letter. The institutional communication must prominently disclose the fact that the Related Performance Information is shown net of the registered fund's fees and expenses and, if applicable, that the registered fund's fees and expenses are lower than those of the Related Accounts.

Posted: 3/9/17

D.3.2. Q. Is the Hartford Letter intended to allow the presentation of Related Performance Information in an institutional communication concerning an actively managed exchange-traded fund ("ETF") that is registered under the Investment Company Act of 1940?

A. Yes. A firm may present Related Performance Information in an institutional communication concerning an actively managed ETF, provided that this presentation is consistent with the representations and conditions contained in the Hartford Letter.

Posted: 3/9/17

D.4. Usability Study and Focus Group Communications

D.4.1. Q. If a firm distributes a communication solely for the purposes of recruiting individuals who might be part of a group to provide feedback or participate in a usability study (through a focus group or otherwise), or solely for the purposes of communicating a "blind" or anonymous survey, must the firm disclose its member name under Rule 2210(d)(3) in the communication?

A. No. Rule 2210(d)(3) expressly states that it does not apply to "blind" advertisements used to recruit personnel. Similarly, it would not apply in these recruiting and feedback situations in which using a member name would counteract the purpose of the communication.

Posted: 1/16/19

D.4.2. Q. If a firm distributes a communication solely to one or more individuals who are engaged to provide feedback concerning the communication or participate in a usability study concerning the communication (through a focus group or otherwise), and those individuals are informed that the communication is being provided solely for such purpose, would that communication be subject to Rule 2210 and its requirements?

A. No.

Posted: 1/16/19

D.5. Use of Hyperlinks in Electronic Communications New

D.5.1. Q. Does FINRA Rule 2210(d)(1)(A) permit a firm to include in electronic communications hyperlinks to content that provides additional information related to the communication in a fair and balanced manner?

A: Yes. FINRA Rule 2210(d)(1)(A) requires firm communications, among other things, to be fair, balanced, and not to omit any material fact or qualification if the omission would cause the communication to be misleading. Consistent with these standards, a firm may rely on a hyperlink to provide additional information or explanations so long as the initial electronic communication that includes the link is itself fair and balanced. For example, a non-misleading electronic communication about opportunities in emerging markets could link to an additional explanation about the basis for a claim in the initial post as well as the risks associated with emerging markets investments. However, a firm may not rely on linked explanations or disclosures to correct a communication that is, on its face false, misleading, exaggerated or promissory. [14] To the extent practicable in the given medium, the link itself, or the text within the communication that introduces the link, should state what will be provided through the link.

Historically, FINRA has interpreted the Communications with the Public Rules to permit hyperlinks to explanations and further information in a variety of situations. For example, FINRA Rule 2210 permits firms to use hyperlinks within banner advertisements to generate interest in a topic and provide more information through hyperlinks, [15] and FINRA has interpreted FINRA Rule 2210 to permit firms to link to required information about testimonials.[16]

This approach is also consistent with the treatment of hyperlinks in the Commission's recently adopted Investment Adviser Marketing rule under the Investment Advisers Act of 1940. [17] The Marketing Rule Adopting Release notes that the rule's use of "fair and balanced" is closely aligned with FINRA Rule 2210's general standards, and that investment advisers may use layered disclosure that employ hyperlinks to meet these requirements. [18]

Posted: 9/30/21

D.6. Internal Rate of Return (IRR) New

D.6.1. Q. Regulatory Notice 20-21 (FINRA Provides Guidance on Retail Communications Concerning Private Placement Offerings) interprets FINRA Rule 2210 to permit the inclusion of an internal rate of return (IRR) if it is calculated in a manner consistent with the Global Investment Performance Standards (GIPS®) adopted by CFA Institute and includes additional GIPS-required metrics such as paid-in capital, committed capital and distributions paid to investors. What is the distinction between calculating IRR in a "manner consistent with the GIPS standards" and "GIPS compliance"?

A. The guidance in *Regulatory Notice 20-21* that IRR be calculated in a "manner consistent with the Global Investment Performance Standards (GIPS)" refers to using the same primary inputs and calculation methodology articulated in the GIPS standards as well as including prominently in the communication the additional required metrics set forth in the GIPS standards. The primary inputs are external cash flows and the period-end value of the investment or terminal value. With respect to the calculation methodology, since-inception IRR can be calculated using common spreadsheet software and the extended IRR (XIRR) function. [19]

Firms that comply with all of the applicable requirements of the GIPS standards on a firm-wide basis may claim compliance with the GIPS standards (i.e., they are "GIPS compliant"). Firms are not required to claim compliance with GIPS or choose to have their firm verified in order to use IRR in private placement communications in a manner that is consistent with the requirements of FINRA Rule 2210.

While the GIPS standards generally prohibit firms from making any statement referring to the calculation methodology as being "in accordance," "in compliance," or "consistent" with the GIPS standards, CFA Institute has created a limited exception for firms and their agents in retail

communications concerning private placement offerings that are prepared in a manner consistent with FINRA Rule 2210 and the guidance in *Regulatory Notice 20-21*. [20]

It is also important to recognize that the requirement to present IRR calculated in a "manner consistent with the Global Investment Performance Standards (GIPS)" only applies to investment programs with ongoing operations that include a combination of realized and unrealized holdings.

When presented in a fair and balanced manner, realized historical performance for a completed investment program, whether expressed as IRR or any other return metric, will generally be consistent with the content standards in FINRA Rule 2210. In contrast, as stated in *Regulatory Notice 20-21*, IRR presented for privately placed new investment programs that have no operations or that operate as a blind pool is a projection prohibited by FIRNA Rule 2210(d)(1)(F).

Posted: 9/30/21

D.6.2. Q. If an investment program has both realized and unrealized holdings, may a firm show returns for each of the realized holdings without also showing the program's IRR?

A. Presenting returns solely for realized holdings in a program with ongoing operations without presenting the fund's IRR may be consistent with FINRA Rule 2210 provided that the information presented is fair and balanced. If a communication shows returns for any realized holding, then returns for each realized holding must be shown with equal prominence. "Cherry picking" or excluding returns for realized holdings that performed poorly would be misleading and inconsistent with FINRA Rule 2210(d)(1)(B).

In contrast, unrealized holdings have no actual performance experience, and any return metric would require its valuation to be estimated. Such metrics would represent a prohibited projection under FINRA Rule 2210(d)(1)(F).

Posted: 9/30/21

D.6.3 Q. May a firm aggregate realized holdings of an investment program together into an "aggregate realized investment" return without showing the total program's IRR?

A. As a general matter, it is misleading for a communication to include metrics that combine or average the performance of only the individual realized holdings. Such metrics may mask unequal or poor returns and the results may not be representative of the ultimate performance of the unrealized holdings or the program as a whole. This is the case whether or not the total fund IRR is included.

Posted: 9/30/21

D.6.4 Q. A firm wants to prepare a communication for an ongoing program that includes an IRR and the additional metrics required by the GIPS standards in accordance with *Regulatory Notice 20-21*. Is the firm allowed to also include information beyond what is required by the GIPS standards?

A. Generally, a firm may include information beyond what is required by the GIPS standards in a communication for an ongoing program. Any information must be presented in a fair and balanced manner, must not be misleading, and otherwise must be consistent with the content standards of FINRA Rule 2210(d).

Posted: 9/30/21

D.7. Prohibition on Predictions or Projections of Investment Performance *New*

D.7.1 Q. May a firm include in a retail private placement communication a "target return" to investors if the communication also includes the assumptions and key risks underlying the return?

A. FINRA Rule 2210(d)(1)(F) prohibits predictions or projections of performance, the implication that past performance will recur, and any exaggerated or unwarranted claim, opinion or forecast. As discussed in Regulatory Notice 20-21, "retail communications may not project or predict ***returns to investors*** such as yields, income, dividends, capital appreciation, percentages or any other future investment performance." This prohibition extends to retail communications that include target returns to investors. However, Regulatory Notice 20-21 makes clear that Rule 2210(d)(1)(F) does not prohibit reasonable forecasts of ***issuer operating metrics*** (e.g., forecasted sales, revenues or customer acquisition numbers) that may convey important information regarding the issuer's plans and financial position, provided that the retail communication provides a sound basis for evaluating the facts as required by Rule 2210(d)(1)(A). Such reasonable forecasts may take the form of target issuer operating metrics, so long as the retail communication does not provide a target return to investors. The Notice also provided guidance on the types of information that should be included, and the factors firms should consider, when creating, reviewing, approving or using forecasts of issuer operating metrics in retail communications.

Posted: 12/8/21

E. Limitations on Use of FINRA's Name

(No Q&As currently under this section)

F. Public Appearances

F.1. Supervision Updated

F.1.1. Q. If a registered representative makes a scripted presentation at a seminar for prospective retail investors, what is the responsibility of the firm with which the representative is associated to supervise the presentation?

A. A sales script used in a seminar is considered a retail communication under FINRA Rule 2210 (assuming the script is used with more than 25 retail investors within a 30 calendar-day period).

The firm with which the representative is associated is responsible for approving prior to use any retail communication used as part of the seminar presentation. If a retail communication is subject to a filing requirement under FINRA Rule 2210, the firm also must file the communication with FINRA. FINRA Rule 2210(f)(3) requires each firm to establish written procedures that are appropriate to its business, size, structure, and customers to supervise its registered representative's public appearance. These procedures must provide for education and training, documentation of such education and training, and surveillance and follow-up to ensure that representatives implement and adhere to the procedures.

Posted: 1/7/13

F.1.2 Q. Our firm's registered representatives may meet with groups either in person or using online conferencing platforms. How should firms supervise these meetings?

A. Firms must supervise registered representatives' live meetings with customer groups, whether in person or through an online conferencing platform, in a manner reasonably designed to achieve compliance with applicable securities laws and regulations and FINRA rules, including FINRA Rule 2210(f). This rule provision sets forth supervision and content standards for public appearances such as seminars, forums, media interviews or other public speaking activities that are unscripted and do not constitute retail communications, institutional communications, or correspondence.

Posted: 9/30/21

F.1.3 Q. If a registered representative uses visual aids, such as a whiteboard or dynamic charts, or a chat or instant messaging feature during a live, unscripted online conference, how should a firm supervise these aspects of the presentation?

A. Depending on the nature and number of persons attending the meeting, the use of these visual aids may be correspondence, retail communications or institutional communications, and the firm must supervise them as such. See FINRA Rules 2210(a), 2210(b) and 3110(b)(4). In addition, their content must be consistent with applicable standards, such as those in FINRA Rule 2210(d).

For example, if a representative meets with fewer than 25 retail investors, and uses the chat feature of the online conferencing platform to answer a live question, that chat content meets the definition of correspondence in FINRA Rule 2210(a)(2). The firm must review the chat content in the same manner as required for supervising and reviewing any other correspondence pursuant to FINRA Rule 3110(b) and 3110.06 through .09.

In another example, if during a meeting that includes more than 25 retail investors, a representative uses the chat feature to post an electronic file containing content that promotes a new mutual fund, the content in the file meets the definition of a retail communication in FINRA Rule 2210(a)(5). Because the content in the file promotes a product of the firm, a registered principal must have approved it prior to use as required by FINRA Rule 2210(b)(1)(A). In addition, because the content in the file promotes a specific registered investment company (i.e., the mutual fund), the firm must also submit it to FINRA's Advertising Regulation Department within 10 business days of first use as required by FINRA Rule 2210(c)(3). In contrast, if during an online meeting that includes more than 25 retail investors, a representative responds to a live audience question by using the platform's whiteboarding feature to draw a diagram illustrating the differences between a conventional bond and a stock, that content would meet the definition of a retail communication in FINRA Rule 2210(a)(5). However, because the representative created and posted the whiteboarding content during an online interactive electronic forum, the firm would not have to approve such content prior to use (see FINRA Rule 2210(b)(1)(D)(ii)). Instead, the firm may review the whiteboarding content in the same manner as required for supervising and reviewing correspondence pursuant to FINRA Rule 3110(b) and 3110.06 through .09.

As a final example, a representative of an ETF broker-dealer distributor hosts a webinar attended by 100 registered representatives of other broker dealers. During the presentation, the distributor representative conducts an interactive poll about the latest ETF offered by the distributor. Once the poll is complete, the distributor representative posts the results live to all of the attendees. Because the audience is composed solely of registered representatives, the poll and the results would meet the definition of institutional communication in FINRA Rule 2210(a)(3). As such, the distributor would need to review the poll and the results in accordance with the firm's written supervisory procedures for the supervision of institutional communications adopted in accordance with FINRA Rule 2210(b)(3). While such procedures don't require review of all institutional communications prior to first use, they must include provisions for the education and training of associated persons as to the firm's procedures governing institutional communications, documentation of such education and training, and surveillance and follow-up to ensure that firm personnel implement and adhere to such procedures.

Posted: 9/30/21

F.1.4 Q. If a third party, such as a fund distributor or program sponsor, presents information or speaks with clients during a presentation, either in person or using an online conferencing platform, during which a representative of a broker-dealer also speaks or presents, what must the representative disclose about that third party?

A. FINRA Rule 2210(f)(1) provides that, when participating in unscripted public appearances, associated persons of broker-dealers must follow the standards of FINRA Rule 2210(d)(1). Paragraph (d)(1)(A) requires firms' communications with the public to be fair and balanced, and prohibits the omission of material information that would cause the communication to be misleading. To comply with these obligations, when a registered representative appears at an event along with personnel from a third party, such as a fund distributor or program sponsor, the representative should clearly explain the purpose of the meeting, the identity of the third-party entity, whether the third-party entity paid for or sponsored the meeting, and the relationship between the representative, the broker-dealer, and the third-party entity. [21]

Posted: 9/30/21

F.1.5 Q. If our registered representatives use communications with the public that direct customers to in-person or online presentations hosted by a third party, what supervision requirements apply?

A. A firm is responsible under FINRA Rule 2210 for third-party content if the firm has adopted or become entangled with such content. [22]

If a firm permits its representatives to direct investors to presentations hosted by a third party that concern securities products or services, FINRA would consider the firm to have adopted that content. Accordingly, the firm would need to ensure compliance with the content and supervision standards addressed above.

In addition, even if a firm or its representatives did not direct customers to attend the third-party hosted presentation, where the firm or representative paid for, arranged for, or was otherwise involved in the presentation, FINRA would consider the firm or representative to be entangled with the presentation. Accordingly, FINRA would treat the presentation as a communication with the public by the firm. 23 Again, under such circumstances, the firm would need to ensure compliance with the content, and supervision standards addressed above.

Posted: 9/30/21

F2. Firm Name

F.2.1. Q. Is a registered representative required to disclose the firm's name during a public appearance?

A. The requirement in FINRA Rule 2210(d)(3) to disclose a firm's name applies to retail communications and correspondence. Accordingly, sales scripts, slide presentations and brochures used in connection with a public appearance must disclose the firm's name. A registered representative is not required to disclose the firm's name as part of non-scripted, extemporaneous remarks during a public appearance.

Posted: 1/7/13

G. SEC Advertising Rules

G.1. SEC Rule 482

G.1.1 Q. Does a promotional item, such as a t-shirt, cap or pen, that contains only the name of a mutual fund or fund family, have to include the prospectus offering legend required by SEC Rule 482 under the Securities Act?

A. No. In FINRA's view, promotional items that only contain the name of a mutual fund or fund family would not be considered an "advertisement" for purposes of Rule 482, and therefore, are not subject to the requirements of that rule, including the requirement to include a prospectus offering legend.

Posted: 5/22/15

G.1.2. Q. Is a communication to a customer that lists the customer's securities and other investments held at a firm, or at various broker-dealers, investment advisers and other entities, and the performance of those investments, subject to Rule 482 or Rule 34b-1 under the Investment Company Act of 1940?

A. No. In FINRA's view, assuming the communication merely informs an existing customer of his or her securities holdings and other investment positions held at the firm or at multiple intermediaries, and the prior performance of those investments, and it does not offer securities of a registered investment company, we believe that the communication would not be considered an advertisement for purposes of Rule 482 and Rule 34b-1. However, if the communication explicitly or implicitly induces the purchase of shares of a registered investment company, we believe that the communication could be subject to the requirements of Rule 482 and Rule 34b-1.

Posted: 5/22/15

---

1. See FINRA Rule 2241(a)(3), (a)(14), (h)(1), (h)(3), and (h)(5).

2. Unless FINRA specifically directs a firm to file its institutional communications pursuant to FINRA Rule 2210(c)(1)(B), a firm is not required to file its institutional communications with the Advertising Regulation Department. If a firm chooses voluntarily to file a third-party research report that qualifies as an institutional communication, however, an appropriately qualified principal must approve the report prior to filing. See FINRA Rule 2210(b)(1)(F).

3. See also letter from Afshin Atabaki, FINRA, to Wallace W. Kunzman, Jr. (December 1, 2014).

4. See FINRA Rule 2210(c)(7)(F).

5. "Responsive web design" refers to technology that changes the display of a web page in response to the needs of users and the devices they're using. The layout may change based on the size and capabilities of the device. For example, on a phone, users would see content shown in a single column view; a tablet might show the same content in two columns. See "Responsive Web Design Basics."

6. Pursuant to FINRA Rule 2210(c)(7)(B), the firm also would not be required to file future versions of the fund fact sheets (such as fact sheets issued after the end of the next calendar quarter) where the changes are limited to updates of more recent statistical or other non-narrative information and non-predictive narrative information that describes market events during the period covered by the communication or factual changes in portfolio composition or is sourced from a registered investment company's regulatory documents filed with the SEC.

7. For example, FINRA has stated that firms are not required to file information, including performance information, provided to participant-directed individual account plan participants pursuant to DOL Rule 404a-5 under ERISA. See Regulatory Notice 12-02 (January 2012).

8. See *Regulatory Notices 07-59 (FINRA Guidance Regarding Review and Supervision of Electronic Communications) and 10-06 (Guidance on Blogs and Social Networking Web Sites)* for additional guidance on supervision of digital correspondence.

9. FINRA Rule 2210(c)(7)(I) excludes from the filing requirements any reprint or excerpt of any article or report issued by a publisher, provided that (i) the publisher is not an affiliate of the member using the reprint or any underwriter or issuer of a security mentioned in the reprint that the member is promoting; (ii) neither the member using the reprint nor any underwriter or issuer of a security mentioned in the reprint has commissioned the reprinted article or report; and (iii) the member using the reprint has not materially altered its contents except as necessary to make the reprint consistent with applicable regulatory standards or to correct factual errors.

10. The SEC staff has taken the position, however, that certain interactive content posted on a real-time electronic forum (i.e., chat rooms or other social media) should be filed under the filing requirements of Section 24(b) of the Investment Company Act of 1940 or Rule 497 under the Securities Act of 1933 (Securities Act), even if it is not required to be filed with FINRA under FINRA Rule 2210. See U.S. Securities and Exchange Commission, Division of Investment Management, IM Guidance Update No. 2013-01 (March 2013).

11. See *Notice to Members 06-48* (September 2006).

12. The Hartford Letter defined "Related Performance Information" as "actual performance of all separate or private accounts or funds that have (i) substantially similar investment policies, objectives, and strategies, and (ii) are currently managed or were previously managed by the same adviser or sub-adviser that manages the registered mutual fund that is the subject of an institutional communication."

13. The Hartford Letter defined "Related Accounts" as all separate or private accounts or funds that fall within the definition of "Related Performance Information."

14. FINRA Rule 2210(d)(1)(B) states, "No member may make any false, exaggerated, unwarranted, promissory or misleading statement or claim in any communication. No member may publish, circulate or distribute any communication that the member knows or has reason to know contains any untrue statement of a material fact or is otherwise false or misleading."

15. The June 1997 Issue of NASD's *Regulatory and Compliance Alert* included an "Ask the Analyst" question and answer regarding banner advertisements. The answer indicated that a banner advertisement that contained a truthful claim regarding mutual funds (and that did not contain promissory language or graphics) could comply with the Rules by hyperlinking to a webpage containing the information necessary to provide a sound basis to evaluate the facts regarding the mutual funds. FINRA has extended this approach to other electronic communications such as interactive social media posts.

16. See *Regulatory Notice 17-18 (Guidance on Social Networking Websites and Business Communications)*.

17. See Investment Advisers Act Rule 206(4)-1(a)(4); see also Investment Advisers Act Release No. 5653 (December 22, 2020), 86 FR 13024 (March 5, 2021) ("Marketing Rule Adopting Release"), codified at 17 CFR 275.206(4)-1.

18. In particular, the Marketing Rule Adopting Release states that, "[s]o long as each layer of a layered advertisement complies with the requirement to provide benefits and risks in a fair and balanced manner, providing hyperlinks to additional content would meet the requirement of [the Rule]." See Marketing Rule Adopting Release, 86 FR at 13044 and note 239.

19. For details, see *Global Investment Performance Standards (GIPS) For Firms* (2020), *GIPS Standards Handbook for Firms* (2020) and *FINRA Regulatory Notice 20-21 and the GIPS Standards* (video).

20. For specific details on the requirements of this limited exception, see Memorandum RE: FINRA's Regulatory Notice 20-21 and References to the GIPS Standards.

21. See *Regulatory Notice 07-43 (Senior Investors)* and *Protecting Senior Investors: Report of Examinations of Securities Firms Providing "Free Lunch" Sales Seminars* for a discussion of effective practices regarding sales seminars.

22. See, e.g., *Regulatory Notice 17-18 (Guidance on Social Networking Websites and Business Communications).*

23. See *Regulatory Notice 10-06 (Guidance on Blogs and Social Networking Web Sites)* for a discussion of the "adoption" and "entanglement" theories as they apply to third-party content.

Frequently Asked Questions Related to Regulatory Relief Due to the Coronavirus Pandemic

Due to the coronavirus pandemic (COVID-19), FINRA is providing temporary relief for member firms from rules and requirements in the Frequently Asked Questions below. The relief provided does not extend beyond the identified rules and requirements. FINRA will continue to monitor the situation to determine whether additional guidance and relief may be appropriate. As coronavirus-related risks decrease, member firms should expect to return to meeting any regulatory obligations for which relief has been provided. When appropriate, FINRA will publish a Regulatory Notice announcing a termination date for the regulatory relief that will provide member firms with time to make necessary operational adjustments.

FINRA has issued a new FAQ that addresses a question regarding the hosting of virtual business entertainment events or meetings that has been asked frequently during the COVID-19 pandemic.

Advertising Regulation

Q. Our firm's registered representatives are unable to meet with their customers face-to-face because they are working from home or due to COVID-19 related restrictions, and instead are meeting with clients via a live video or audio conferencing platform. How should our firm supervise these meetings? Is the firm required to keep records of these live video meetings?

A: Members must supervise registered representatives' live meetings with customers via video or audio conferencing platforms in a manner reasonably designed to achieve compliance with applicable securities laws and regulation and FINRA rules.

Unless required to record pursuant to FINRA Rule 3170 (Tape Recording of Registered Persons by Certain Firms) or otherwise, members generally are not required to record live video or audio conferences with customers. However, if a registered representative during the video or audio conference uses the chat or instant messaging feature of the platform or presents slides or other written (including electronic) communications, the member must keep records of these written communications in accordance with Securities Exchange Act Rule 17a-4 and FINRA Rules 3110.09 (Supervision) and 4511 (General Requirements), and their content must be consistent with applicable standards such as FINRA Rule 2210 (Communications with the Public) and 3110(b) (Supervision). Depending on the nature and number of persons attending the video meeting, these written communications may be correspondence, retail communications or institutional communications, and must be supervised as such. See FINRA Rules 2210(b) and 3110(b)(4).

Moreover, if a member chooses to record live video or audio conversations with customers, the member may be required to produce the recording in connection with a regulatory request. If a firm permits public appearances through video or audio conferencing platforms, the member must ensure compliance with FINRA Rule 2210(f).

Added April 16, 2020

Q: What steps should members consider regarding communicating with customers?

A: As discussed in Regulatory Notice 20-08, FINRA understands that members may experience significantly increased customer call volumes or online account usage during a pandemic (e.g., due to significant market movements), which may cause temporary operational challenges. Members are encouraged to review their BCPs regarding communicating with customers and ensuring customer access to funds and securities during a significant business disruption.

If registered representatives are unavailable to service their customers, members are encouraged to promptly place a notice on their websites indicating to affected customers who they may contact concerning the execution of trades, their accounts, and access to funds or securities. Supervisory control policies and

procedures should be considered that will mitigate risks that may arise due to the reduced ability to communicate with customers, inability to rely on mail or other disruption to the existing controls over communications with customers.

Added March 24, 2020

Q: Is my firm required to file non-promotional communications with FINRA?

A: No. FINRA Rule 2210(c)(7) (Communications with the Public) excludes from Rule 2210's filing requirement retail communications that do not make any financial or investment recommendation or otherwise promote a product or service of the member. For example, a member is not required to file with FINRA a retail communication regarding COVID-19 that does not make any financial or investment recommendation or promote a product or service of the member.

Additional information on exclusions from Rule 2210's filing requirement are included in FINRA Advertising Regulation Department's dedicated FAQs. Members with additional questions may also contact the FINRA Advertising Regulation Department ((240) 386-4500 or finra_adv@finra.org).

Added March 24, 2020

Regulatory Notice 20-14

Oil-Linked Exchange-Traded Products

Sales Practice Obligations With Respect to Oil-Linked Exchange-Traded Products

May 15, 2020

Notice Type
- Guidance

Suggested Routing
- Legal and Compliance
- Registered Representatives
- Retail
- Senior Management

Key Topics
- Communications with the Public
- Oil-Linked Exchange-Traded Products
- Suitability
- Supervision
- Training

Referenced Rules & Notices
- FINRA Rule 2111
- FINRA Rule 2210
- FINRA Rule 3110
- Notice to Members 05-26
- Regulatory Notice 09-31
- Regulatory Notice 10-51
- Regulatory Notice 12-03
- Regulatory Notice 17-32
- SEC Regulation Best Interest

Summary

Exchange-traded products (ETPs) provide different types of exposure to the oil market through several product structures, which some investors or investment professionals might not understand.[1] Moreover, the performance of such products may be linked to unfamiliar indices or reference benchmarks, making them difficult for the average investor to comprehend. In particular, a number of these ETPs are designed to track daily price movements of specified crude oil futures contracts, such as those on West Texas Intermediate (WTI) light, sweet crude oil (referred to herein as "oil-linked ETPs").[2] Due to recent extraordinary conditions in crude oil markets, combined with the manner in which the products are structured, several oil-linked ETPs have experienced significant volatility and lost a substantial percentage of their value, with at least one ETP liquidating and another forced to halt the issuance of new shares and adjust its investment objective.

These concerns are not limited to oil-linked ETPs: some other commodity-linked products, such as natural gas ETPs, as well as volatility-linked ETPs, may share similar features and have been the subject of prior FINRA guidance and regulatory action.[3] Based on FINRA's experience with complex products broadly, some investors—as well as investment professionals recommending them—may not understand oil-linked ETPs' investment objectives, how their performance relates to the "spot" (or cash) price of oil, or how the different product structures can impact their performance and the investor experience.[4]

This *Notice* reminds firms of their sales practice obligations in connection with oil-linked ETPs, including that recommendations to customers must be based on a full understanding of the terms, features, and risks of the product recommended; communications with the public must be fair and accurate; firms must have reasonably designed supervisory procedures in place to ensure that these obligations are met; and firms that offer oil-linked ETPs must train registered representatives who sell these products about the terms, features and risks of these products.

Questions concerning this *Notice* should be directed to:

- Joseph P. Savage, Vice President, Office of General Counsel, at (240) 386-4534 or by email at *joe.savage@finra.org*;
- Amy Sochard, Vice President, Advertising Regulation, at (240) 386-4508 or by email at *amy.sochard@finra.org*; or
- Richard Vagnoni, Senior Economist, Office of Financial Innovation, at (202) 728-6934 or by email at *richard.vagnoni@finra.org*.

Background and Discussion

Given the practical difficulties of investing directly in commodities such as oil, commodity-linked ETPs often track commodity futures or futures indices rather than the underlying spot commodity. As with other commodity-linked ETPs, such as those linked to natural gas, oil-linked ETPs generally provide exposure to the price of oil by tracking oil futures through two different ETP structures—ETNs and commodity pools.

Oil-linked ETNs, which are debt obligations of an issuer and do not hold any underlying portfolio, promise to pay the note holder a return linked to the performance of an index at note maturity. ETN issuers have significant discretion in the creation (*i.e.,* issuance) of new notes as well as note redemption (*e.g.,* early termination), which can impact the performance that a note holder experiences and the extent to which the market price of the note reflects its value.[5]

In contrast to ETNs, commodity pools do hold an underlying portfolio of futures (or other commodity interests). While similar to ETFs, a commodity pool ETP has unique structural features that can introduce additional risks. For example, a commodity pool ETP must update its registration statement with the SEC once every three years and must file a new registration statement for new shares if the existing share limit under the effective registration statement is reached. An ETP structured as a commodity pool also may be subject to position limits in terms of the number of futures contracts that it may hold or issues related to margin. These features can limit the ETP's ability to create shares, which can result in a tendency for the ETP's market price to deviate from the underlying value of the ETP, or cause the ETP to change investment holdings (*e.g.,* using different futures contracts or swaps).

As lockdowns related to the coronavirus disease (COVID-19) remain in force, oil demand has declined precipitously and excess storage capacity has reportedly decreased significantly as well, pushing crude oil prices to record lows. Recently the June 2020 WTI crude oil futures contract fell 43 percent to close at $11.57 per barrel—only one day after the expiring May 2020 WTI contract price dropped below zero and settled at *minus* $37.63 per barrel.[6] This plunge in market value has significantly impacted ETPs tracking WTI futures.

For example, as of April 22, 2020, the largest oil-related ETP had lost 41 percent of its value in one week. This ETP also subsequently adjusted its investment focus from near-dated futures to longer-dated contracts.[7] Reports suggest that retail investors have been investing in oil-linked ETPs during this volatile period. Surging investor demand for this oil-linked ETP in particular led to a dramatic increase in new share issuance, which ultimately exhausted the number of available shares permitted to be issued under the ETP's existing registration statement.

As a result, this ETP was unable to issue new shares until a new registration statement was filed with the SEC and became effective. With its normal share creation mechanism non-operational, there have been significant variations between the market price at which shares are traded and the shares' net asset value.

Separately, the issuer of another oil-related ETN tracking WTI futures announced an early liquidation.[8] Leveraged and inverse oil-linked ETPs that seek to deliver multiples or the opposite of the return of an oil-linked index likewise have been extremely volatile during these market conditions.

Experience with similar complex products suggests that some retail investors and investment professionals recommending oil-linked ETPs, including commodity pools and ETNs, may have mistakenly thought that these ETPs are a proxy for the spot price of oil, when in fact their investment objectives are to track oil futures contracts.[9] Rather than tracking the spot price, oil-linked ETPs generally provide exposure to oil by tracking short-term or other oil futures or futures indices. These ETPs may track or hold futures contracts on a rolling basis, meaning that they will replace shorter-term contracts or contracts about to expire with contracts that have more distant or deferred expiration dates in order to maintain the desired exposure.

An ETP whose objective is to provide exposure to the near-month futures contract may roll out of the near-month contract as it approaches expiration and into the next-month contract over a series of days. If the prices of futures contracts with more distant expiration dates are higher than those with shorter dates, the market is often said to be in "contango." Other things being equal, rolling out of shorter-term contracts into longer-term contracts in such a market can lead to losses. If the opposite is true, the market is often said to be in "backwardation," and rolling out of shorter-term contracts into longer-term contracts can lead to gains.

The oil futures market has experienced both periods of backwardation and contango over the last decade. Over longer time horizons, these features of the futures market can be a factor that leads to a divergence in the performance of a futures-linked ETP and that of the spot commodity, and in some cases that divergence can be significant. Recently, the oil futures market has been in "super-contango," as oil storage capacity has diminished, which can exacerbate losses to investors who hold oil-linked ETPs for extended periods of time.

Sales Practice Obligations

Over the years, FINRA has published guidance to firms about the risks of recommending complex products, such as oil-linked ETPs, to retail customers, particularly buy-and-hold retail investors with an intermediate- or long-term time horizon. *Regulatory Notice 10-51* reminded firms of their sales practice obligations with regard to commodity futures-linked securities.[10] That *Notice* discussed the volatility of oil prices and the risk that commodity futures-linked securities can perform differently than the spot price for the commodity itself, which can lead to unexpected results for investors who do not understand the product or who mistakenly believe the product will replicate the performance of the commodity's spot price. *Regulatory Notice 12-03* addressed similar issues in the context of complex products generally.[11]

As detailed in *Regulatory Notice 12-03*, investments tied to the performance of securities, indices, commodities or markets that may not be well known or well understood by investors, such as oil-linked ETPs, are "complex" products. Firms should review *Regulatory Notice 12-03* and consider whether to use the type of heightened scrutiny and supervision suggested therein for these complex products.[12] Firms are similarly reminded that they must comply with the obligations discussed below when offering oil-linked ETPs.

Suitability and Regulation Best Interest

FINRA Rule 2111 (Suitability) requires a firm or associated person making a recommendation to have a reasonable basis to believe that the recommended transaction or investment strategy involving a security or securities is suitable for the customer, based on the information obtained through the reasonable diligence of the member or associated person to ascertain the customer's investment profile. Two of the main suitability obligations delineated in Rule 2111 that are particularly relevant to oil-linked ETPs are customer-specific and reasonable-basis suitability.

Customer-specific suitability requires a firm or its associated persons to have a reasonable basis to believe that a recommendation is suitable for a particular customer based on the customer's investment profile, including the customer's investment experience, risk tolerance, liquidity needs, investment objectives, and financial situation and needs.[13] For example, depending on the facts and circumstances, an oil-linked ETP might be suitable for an experienced customer with a speculative investment objective, but it likely would not be suitable for a less experienced customer or a customer with a more conservative or a buy-and-hold investment objective.

Reasonable-basis suitability requires that the firm or associated person recommending a securities transaction or investment strategy involving securities perform reasonable diligence to understand the nature of that transaction or strategy, as well as potential risks, and then determine whether there is a reasonable basis to believe, based on the reasonable diligence, that the recommendation is suitable for at least some investors. The level of reasonable diligence that is required will rise with the complexity and risks associated with the transaction or strategy.

With regard to a complex product such as an oil-linked ETP, an associated person should be capable of explaining, at a minimum, the product's main features and associated risks.[14] These would include, for example, understanding generally how products tracking futures contracts or futures indices work, how contango and backwardation may affect their performance, and how such products may perform relative to the spot asset (*e.g.,* oil), especially over extended periods of time.

Oil-linked ETPs may employ various strategies (*e.g.,* focusing on short-term futures versus more diversified exposure), so understanding the differences among the various offerings is important as well. Some products are designed to be used more tactically—on a shorter-term basis—such as geared (*i.e.,* leveraged or inverse) ETPs, and such products would be particularly unsuitable for customers intending to buy and hold securities. An associated person should understand the differences in product structures (*e.g.,* commodity pool versus ETN) and how the structural features of different ETPs may present additional risks (*e.g.,* suspension of new issuance or accelerated termination).

Starting on June 30, 2020, recommendations of securities, including oil-linked ETPs, to retail customers will be governed by SEC Regulation Best Interest ("Reg BI").[15] Reg BI enhances firms' standard of conduct beyond existing suitability obligations by, among other things, requiring firms to act in the retail customer's best interest at the time the recommendation is made, without placing the financial or other interests of the firm ahead of the interests of the retail customer.[16] Firms should ensure that any recommendations of oil-linked ETPs made after the compliance date comply with their Reg BI obligations.

Communications with the Public

FINRA Rule 2210 (Communications with the Public) requires, among other things, that all communications with the public be based on principles of fair dealing and good faith, be fair and balanced, and provide a sound basis for evaluating the facts in regard to any particular security or type of security, industry or service. Communications regarding oil-linked ETPs that present the benefits of the products must be balanced by a clear description of the risks, and may not omit any material fact or qualification that would cause such a communication to be misleading. For example, communications that present the benefits of oil-linked ETPs must include key risks such as the inherent fluctuations of oil prices and the speculative nature of futures investments, and must explain clearly that the ETP's price will not track directly the spot price of oil.

Communications that present the benefits of oil-linked ETPs or other investments that rely on futures must explain how the investment may be impacted by contango and backwardation. Further, communications concerning an ETP that is designed to achieve its investment objective on a short-term basis (*e.g.,* daily) must state that fact and specifically disclose that the ETP is not designed to, and will not necessarily, track the underlying index or benchmark over a longer period of time. FINRA reminds firms that providing risk disclosure in a separate document such as a prospectus does not cure otherwise deficient disclosure in sales material, even if the sales material is accompanied or preceded by the prospectus.

Supervision

FINRA Rule 3110 (Supervision) requires that firms establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules. A reasonably designed system must be tailored specifically to a member's business, taking into account among other things, the nature and complexity of the products offered and the customer base.

Oil-linked ETPs are complex products that could be easily misunderstood and improperly sold by registered representatives. As discussed in *Regulatory Notice 12-03* and noted above, firms should consider whether to use heightened scrutiny and supervision of these ETPs. Firms must act reasonably to ensure that their registered representatives and supervisors understand the risks presented by such products.

Training

Firms that offer oil-linked ETPs must train registered persons about the terms, features and risks of these products, as well as the factors that would make such products either suitable or unsuitable for certain investors, particularly retail investors.[17] Training should emphasize the need to understand and consider the risks associated with such products, including the investor's time horizon, and the impact of time and volatility on the ETP's performance. Training should emphasize that, due to the complexity and structure of these products, they may not perform over time in direct correlation to their underlying index or benchmark. Additionally, when recommending complex products such as oil-linked ETPs, firms and associated persons should consider whether less complex or less costly products could achieve the same objective for their customers.

Conclusion

Oil-linked ETPs are complex products that may not be suitable for some investors, such as retail investors with conservative investment objectives and long time horizons. Given the heightened risks that these products raise, firms must be diligent in ensuring that their sales of these products are consistent with the requirements under the suitability, communications and supervision rules, and beginning on June 30, 2020, their obligations under Reg BI, as well as other applicable rules and requirements. Firms are reminded of their obligation to put reasonably designed supervisory controls in place, and to train their registered representatives and supervisors to ensure that suitability and other obligations under FINRA and SEC rules are met.

Endnotes

1. An ETP is a security listed on an exchange that seeks to provide exposure to the performance of an index, benchmark, or actively-managed strategy. The most common type of ETP is the exchange- traded fund (ETF). ETFs are registered under the Investment Company Act of 1940 (1940 Act), and are organized under the laws used for the issuance and governance of mutual funds. Other ETPs, which are not registered under the 1940 Act, include commodity pools, which invest in futures, grantor trusts, which hold physical commodities or currencies, and exchange-traded notes (ETNs), which track an index or benchmark but are debt obligations of an issuer and hold no underlying portfolio. While ETPs are often referred to as exchange-traded "funds" or "ETFs," there are important differences among the various legal or tax-related structures that are used across the product range—and such differences have implications for investors and product issuers. All ETPs are registered under the Securities Act of 1933 and Securities Exchange Act of 1934, but different ETPs may be subject to different regulatory requirements and oversight by different Securities and Exchange Commission (SEC) divisions or the Commodity Futures Trading Commission depending on their particular structures. Moreover, there is no universally-accepted comprehensive naming framework for the products. Differences among the various ETP structures include the asset classes in which portfolios may invest, how portfolios are constructed, use of derivatives and securities lending, when and if distributions are reinvested, and how taxes are assessed.
2. For the purposes of this *Notice*, "oil-linked ETPs" include ETPs that seek to provide exposure to oil as an asset as represented by investments in exchange-traded crude oil futures contracts and ETNs that are designed to provide exposure to an oil-linked futures price index.
3. *See, e.g.*, *Regulatory Notice 10-51* (October 2010) (Sales Practice Obligations for Commodity Futures-Linked Securities) and *Regulatory Notice 17-32* (October 2017) (FINRA Reminds Firms of Sales Practice Obligations for Volatility-Linked Exchange-Traded Products).
4. *See* Cadaret, Grant & Co., Inc., Securities Act Release No. 10542, 2018 SEC LEXIS 2239 (Sept. 11, 2018).
5. For a discussion of the risks of investing in ETNs, including the risk of early termination, *see* FINRA Investor Alert, "Exchange-Traded Notes – Avoid Unpleasant Surprises" (July 10, 2012).
6. *See* "Collapse in Oil Prices Deepens, Dragging Down Markets Globally," *The Wall Street Journal*, April 22, 2020, p. A1.
7. *See* "Oil Wagers Burn Some Individual Investors," The Wall Street Journal, April 22, 2020, p. B1.
8. *See* "Oil Wagers Burn Some Individual Investors," *The Wall Street Journal*, April 22, 2020, p. B13; *see also* Barclays press release, "Barclays announces the redemption of the iPath® Series B S&P GSCI® Crude Oil Total Return Index ETNs (the "ETNs") and the suspension of further sales and issuance of the ETNs," (April 20, 2020).
9. *See* Kate Rooney, "Young investors rush into struggling oil ETF that isn't even tracking the price of oil anymore" (April 23, 2020), available at www.cnbc.com.

10. *See* Regulatory Notice 10-51 (October 2010) (Sales Practice Obligations for Commodity Futures-Linked Securities). Notice 10-51 addressed firms' obligations with regard to suitability, communications with the public, supervision and training.

11. *See* Regulatory Notice 12-03 (January 2012) (Heightened Supervision of Complex Products).

12. *See id*.

13. A customer's investment profile also includes the customer's age, other investments, tax status, investment time horizon, and any other information the customer may disclose to the member or associated person in connection with such recommendation. *See* FINRA Rule 2111(a).

14. FINRA notes, as well, the importance of vetting of new products, particularly new products that are complex or have potentially high levels of risk associated with them. *See, e.g.,* Regulatory Notice 05-26 (April 2005) (NASD Recommends Best Practices for Reviewing New Products) (highlighting best practices for vetting new products), and Regulatory Notice 09-31 (June 2009) (FINRA Reminds Firms of Sales Practice Obligations Relating to Leveraged and Inverse Exchange-Traded Funds) (concerning the obligation to vet new complex and non-traditional ETFs).

15. 17 CFR 240.15l-1; *see also* Securities Exchange Act Release No. 86031 (June 5, 2019), 84 FR 33318 (July 12, 2019).

16. Under Reg BI, a "retail customer" is a natural person or the legal representative of the natural person, who (i) receives a recommendation of any securities transaction or investment strategy involving securities from a broker, dealer, or a natural person who is an associated person of a broker or dealer, and (ii) uses the recommendation primarily for personal, family, or household purposes. 17 CFR 240.15l-1(b)(1). A retail customer may include a natural person who falls within the definition of "institutional account" under FINRA Rule 4512(c) (*e.g.,* a natural person with total assets of at least $50 million), and thus previously was excluded from the customer-specific suitability requirements of FINRA Rule 2111 under specified conditions.

17. *See* Notice to Members 05-26 (April 2005) (NASD Recommends Best Practices for Reviewing New Products).

Regulatory Notice 20-21

Communications With the Public

FINRA Provides Guidance on Retail Communications Concerning Private Placement Offerings

July 1, 2020

Notice Type
- Guidance

Suggested Routing
- Advertising
- Compliance
- Corporate Financing
- Legal
- Operations
- Registered Representatives
- Senior Management

Key Topics
- Communications with the Public
- Private Placements
- Retail Communications

Referenced Rules
- FINRA Rule 2210
- Regulation D
- Regulatory Notice 10-22
- Regulatory Notice 13-18
- Regulatory Notice 19-31

Summary

This *Notice* provides guidance to help member firms comply with FINRA Rule 2210, Communications with the Public, when creating, reviewing, approving, distributing, or using retail communications concerning private placement offerings.

Questions concerning this *Notice* should be directed to:

- Amy C. Sochard, Vice President, Advertising Regulation, at (240) 386-4508; or
- Ira D. Gluck, Director, Advertising Regulation, at (240) 386-4614.

Background and Discussion

Private Placement Offerings

Private placements are unregistered, non-public securities offerings that rely on an available exemption from registration with the Securities and Exchange Commission (SEC) under either Sections 3 or 4 of the Securities Act of 1933 (Securities Act).[1] Most private offerings, however, are sold pursuant to one of three "safe harbors" under Rules 504, 506(b), and 506(c) of Securities Act Regulation D (Reg D).[2]

Reg D requires companies and funds to file a Form D through the SEC's EDGAR system when selling unregistered securities based on a claimed Reg D exemption. The most recent Reg D data published by the SEC's Division of Economic and Risk Analysis indicates that issuers make approximately 20,000 new offering Reg D filings with the SEC each year.[3] Of this total, approximately 4,000 new offerings identify an "intermediary," such as a broker or finder, as participating in an offering.

Private placements sold by FINRA member firms to individuals generally must be filed with FINRA. In this regard, FINRA Rules 5122 and 5123 require a member firm to file offering documents regarding specified private placements in which the member firm participates.[4] FINRA receives

approximately 2,000 new offering filings from its member firms each year,[5] and uses analytics and trained analysts to conduct a risk-based review of each filing. The number of annual filings with FINRA indicates that approximately half of the Reg D filings identifying intermediaries are for offerings by entities that are not subject to FINRA rules or offerings by member firms that are not required to file under Rules 5122 or 5123.

The offerings that are sold directly by issuers or through the efforts of intermediaries that are not FINRA member firms are not subject to the regulatory requirements applicable under FINRA rules and are not subject to FINRA's examination and review programs. Although FINRA does not have jurisdiction over Reg D private placements that are sold directly to investors or through non-member firm intermediaries, it is committed to promoting investor protection through meaningful regulation and oversight of member firms participating in these offerings.

The remainder of this *Notice* addresses the subset of private placements conducted by member firms.

Private Placement Retail Communications

Many private placement offerings to retail investors include marketing or sales communications that meet the definition of retail communication in Rule 2210(a)(5).[6] For example, FINRA has observed that more than 40 percent of the offerings filed pursuant to FINRA Rule 5123 include retail communications. In addition, the adoption of Rule 506(c) under Reg D eliminated the prohibition against general solicitation and advertising for private placement offerings where all purchasers of the securities are verified accredited investors. Consequently, member firms have become increasingly involved in the distribution of private placement securities through online platforms and other widely disseminated communications such as digital advertisements.[7]

FINRA Rule 2210(d)(1) requires that all member firm communications be fair, balanced and not misleading. Communications that promote the potential rewards of an investment also must disclose the associated risks in a balanced manner.[8] In addition, communications must be accurate and provide a sound basis to evaluate the facts with respect to the products or services discussed. Rule 2210(d)(1) also prohibits false, misleading or promissory statements or claims, and prohibits the publication, circulation or distribution of a communication that a member firm knows or has reason to know contains any untrue statement of a material fact or is otherwise false or misleading. With few exceptions, Rule 2210(b)(1) requires that an appropriately registered principal approve each retail communication before the earlier of its use or filing with FINRA's Advertising Regulation Department.[9]

Recent FINRA reviews of retail communications concerning private placements have revealed deficiencies. For instance, most if not all investments in private placements are illiquid, and many such investments are speculative in nature. Some retail communications do not balance claims of these investments' benefits by disclosing these risks. Others have contained false, misleading, or promissory statements or claims such as assertions about the likelihood of a future public offering of the issuer, claims about the future success of the issuer's new or untried business model, inaccurate or misleading assertions concerning the regulation or relative risk of the offering, or predictions or projections of investment performance prohibited by FINRA Rule 2210(d)(1)(F).

FINRA is providing the following guidance to assist member firms in their creation, review, approval, distribution or use of retail communications concerning private placement securities.

Third-Party Prepared Materials

Rule 2210(a)(5) defines "retail communication" as "any written (including electronic) communication that is ***distributed or made available*** to more than 25 retail investors within any 30 calendar-day period."[10] FINRA disciplinary actions demonstrate that member firms can be liable for violations of Rule 2210 when distributing or using noncompliant retail communications prepared by a third party.[11]

Regulatory Notice 10-22 states that "[a member firm] that assists in the preparation of a private placement memorandum or other offering document should expect that it will be considered a communication with the public by that [member firm] for purposes of ... Rule 2210, FINRA's advertising rule. If a private placement memorandum or other offering document presents information that is not fair and balanced or that is misleading, then the [member firm] that assisted in its preparation may be deemed to have violated ... Rule 2210." *Notice 10-22* also provides that "sales literature concerning a private placement that a [member firm] distributes will generally be deemed to constitute a communication by that [member firm] with the public, whether or not the [member firm] assisted in its preparation."

In addition, FINRA has observed that some issuer-prepared private placement memoranda (PPMs) are bound or presented as one electronic file with retail communications, such as cover pages or exhibits. Such retail communications are distinguishable by their marketing or promotional content from the factual descriptions and financial information about the issuer generally disclosed in the PPMs. Regardless of whether a member firm distributes a retail communication that is attached to a PPM or as a standalone document, it constitutes a communication of the member firm subject to Rule 2210.

Balanced Presentation of Risks and Investment Benefits

Rule 2210 requires communications that discuss the benefits of an investment also to include a discussion of its risks.[12] As indicated above, retail communications that discuss the potential benefits of investing in private placements should balance this discussion with disclosure of their risks, such as the potential for private placement investments to lose value, their lack of liquidity and their speculative nature. Providing risk disclosure in a separate document, such as a PPM, or in a different section of a website does not substitute for disclosure contained in or integrated with retail communications governed by Rule 2210.

Retail communications often highlight the business of the issuer and discuss the value proposition of a potential investment. In such cases, the key risks associated with an investment in the issuer are necessary in order to balance the positive portrayal of the investment. For example, when the issuer is a startup company, the risks may include a limited track record; more experienced or larger competitors; overreliance on financing; reliance on a single supplier, customer or employee; or lack of management experience.

Reasonable Forecasts of Issuer Operating Metrics

Rule 2210(d)(1)(F) generally prohibits the use of any prediction or projection of performance, as well as any exaggerated or unwarranted claim, opinion or forecast.[13] Accordingly, retail communications concerning private placements may not project or predict ***returns to investors*** such as yields, income, dividends, capital appreciation percentages or any other future investment performance.

However, FINRA would not consider reasonable forecasts of ***issuer operating metrics*** (*e.g.*, forecasted sales, revenues or customer acquisition numbers) that may convey important information regarding the issuer's plans and financial position to be inconsistent with the rule. Presentations of reasonable forecasts of issuer operating metrics should provide a sound basis for evaluating the facts as required by Rule 2210(d)(1)(A). For example, such presentations should include clear explanations of the key assumptions underlying the forecasted issuer operating metrics and the key risks that may impede the issuer's achievement of the forecasted metrics.

When creating, reviewing, approving, distributing or using forecasts of issuer operating metrics in retail communications, member firms should consider:

I. the time period forecasted (generally a time period in excess of five years would be unreasonable);

II. whether growth rate assumptions are commensurate with the nature and scale of the business;

III. whether forecasted gross margins[14] are commensurate with industry averages; and

IV. whether sales and customer acquisition forecasts are reasonable in relation to the overall market for the issuer's products or services.

While sources of contractual revenue such as royalty or master lease agreements may inform or provide a basis for reasonable forecasts of issuer operating metrics, it would be inconsistent with Rule 2210(d)(1)(B) to characterize specific revenue or cash flow as guaranteed or certain. Moreover, Rule 2210(d)(1)(F) precludes member firms from using the data from forecasts of issuer operating metrics to project or depict specific investment returns to an investor.

Distribution Rates

Regulatory Notice 13-18 provided guidance to member firms regarding communications with the public for registered and unregistered real estate investment programs. Given that some non-real estate private placement investments employ similar structures, the principles relating to distribution rates contained in that *Notice* are applicable to retail communications regarding private placement investments designed to provide distributions to investors and are reiterated below.

Some issuers fund a portion of their distributions through return of principal or loan proceeds. For example, a portion of a newer program's distributions might include a return of principal until its assets are generating significant cash flows from operations. Consistent with Rule 2210(d)(1)(B)'s prohibition of false, exaggerated, unwarranted, promissory or misleading claim, member firms must not misrepresent the amount or composition of such distributions. Nor may member firms state or imply that a distribution rate is a "yield" or "current yield" or that investment in the program is comparable to a fixed income investment such as a bond or note. Presentations of distribution rates consistent with Rule 2210 would disclose:

- that distribution payments are not guaranteed and may be modified at the program's discretion;
- if the distribution rate consists of return of principal (including offering proceeds) or borrowings, a breakdown of the components of the distribution rate showing what portion of the quoted percentage represents cash flows from the program's investments or operations, what portion represents return of principal, and what portion represents borrowings;
- the time period during which the distributions have been funded from return of principal (including offering proceeds), borrowings or any sources other than cash flows from investment or operations;
- if the distributions include a return of principal, that by returning principal to investors, the program will have less money to invest, which may lower its overall return; and
- if the distributions include borrowed funds, that since borrowed funds were used to pay distributions, the distribution rate may not be sustainable.[15]

FINRA believes that it is inconsistent with Rule 2210(d)(1) for retail communications to include an annualized distribution rate until the program has paid distributions that are, on an annualized basis, at a minimum equal to that rate for at least two consecutive full quarterly periods.[16]

Internal Rate of Return

Internal Rate of Return (IRR) is a measure of performance commonly used in connection with marketing private placements of real estate, private equity and venture capital. IRR shows a return earned by investors over a particular period, calculated on the basis of cash flows to and from investors (*i.e.,* the percentage rate earned on each dollar invested for each period the dollar was invested). IRR is calculated as the discount rate that makes the net present value of all cash flows from an investment equal to zero.[17]

A drawback of IRR calculations is their inherent assumption that investors will be able to reinvest any distributions from the investment at the IRR rate. In practice, it is unlikely that this would occur. Another drawback is that in order to calculate IRR for a portfolio that includes holdings that have not yet been sold (or otherwise liquidated or matured), a valuation of those remaining assets must be estimated. Depending on the nature of the asset, these estimated values may be based on subjective factors and assumptions.

The use of IRR in retail communications concerning privately placed new investment programs that have no operations or that operate as a blind pool would be inconsistent with the prohibition on unwarranted forecasts or projections in Rule 2210(d)(1)(F).

Nevertheless, FINRA interprets Rule 2210 to permit retail communications to include IRR for completed investment programs (*e.g.,* the holding matured or all holdings in the pool have been sold). In addition, FINRA does not view as inconsistent with the rule retail communications that provide an IRR for a specific investment in a portfolio if the IRR represents the actual performance of that holding.

Investment programs such as private equity funds and REITs may have a combination of realized investments and unrealized holdings in their portfolios. Where the program has ongoing operations, FINRA interprets Rule 2210 to permit the inclusion of IRR if it is calculated in a manner consistent with the Global Investment Performance Standards (GIPS) adopted by the CFA Institute and includes additional GIPS-required metrics such as paid-in capital, committed capital and distributions paid to investors.[18]

Endnotes

1. *See* 15 U.S.C. 77c and 77d.
2. *See* 17 CFR 230.504, 230.506(b) and 230.506(c).
3. *Capital Raising in the U.S.: An Analysis of the Market for Unregistered Securities Offerings, 2009-2017:* https://www.sec.gov/dera/staff-papers/white-papers/dera_white_paper_regulation_d_082018.
4. Rules 5122 and 5123 provide exemptions from the filing requirement when certain types of securities are sold or securities are sold to certain types of investors. For example, member firms are not required to file offerings made pursuant to Securities Act Rule 144A or Regulation S, or offerings sold solely to institutional accounts as defined in FINRA Rule 4512(c). *See* Rules 5122(c) and 5123(b). As a result of these exemptions, both rules apply predominately to retail private placements.
5. The total for "new offering filings" excludes duplicate filings for the same offering by different member firms.
6. "Retail communication" means any written (including electronic) communication that is distributed or made available to more than 25 retail investors within any 30 calendar-day period.
7. *See* FINRA's 2019 Annual Risk Monitoring and Examinations Priorities Letter (January 2019). The letter discusses factors FINRA may consider in reviewing online distribution platforms.
8. *See Regulatory Notice 19-31* (September 19, 2019), Question 3 ("FINRA rules require that communications be fair and balanced, but don't require them to be exhaustive lists of all possible risks and warnings associated with a product or service. Information about risks, costs or drawbacks is more effective when it is related to the benefits that the communication promotes.").
9. For example, pursuant to Rule 2210(b)(1)(C), if a member firm has already filed a retail communication with FINRA's Advertising Regulation Department and received a letter indicating that such communication appears to be consistent with applicable standards, another member firm may use that communication without having a principal approve it, provided the communication is not materially altered or used in a manner that is inconsistent with the department's letter.
10. Emphasis added. Rule 2210's definitions of correspondence and institutional communications also refer to communications that are "distributed or made available" to particular investors. *See* FINRA Rules 2210(a)(2) and (a)(3).
11. *See e.g., Phillipe N. Keyes*, 89 S.E.C. 792, 800 (2006), *Sheen Financial Resources, Inc.,* Exchange Act Release No. 35477, 52 SEC 185, SEC LEXIS 613 (1995), Fidelity Brokerage Services LLC, Letter of Acceptance, Waiver and Consent No. 2008013056101 (2011) or HSBC Securities (USA) Inc., Letter of Acceptance Waiver and Consent No 008013863801 (2010).
12. *See* FINRA Rule 2210(d)(1)(D).
13. Rule 2210(d)(1)(F) contains three exceptions from this prohibition, subject to specified conditions: (1) hypothetical illustrations of mathematical principles; (2) investment analysis tools and reports generated by such tools; and (3) a price target contained in a research report.
14. Gross margin represents the percent of total sales revenue that the company retains after incurring the direct costs associated with producing the goods and services sold by a company. *See Jay Michael Fertman*, 51 SEC 943,950 (1994) and *Excel Fin., Inc.,* 53 SEC 303, 311-12 (1997).

15. *See* *Regulatory Notice 13-18* (May 2013).

16. *Id.* "In order to be fair and balanced, firm communications concerning a real estate program may not include an annualized distribution rate until the program has paid distributions that are, on an annualized basis, at a minimum equal to that rate for at least two consecutive full quarterly periods."

17. IRR is also known as money-weighted returns. This can be contrasted to a time-weighted return, which is the compounded growth rate of $1 over the time period. Average annual total returns used by mutual funds pursuant to SEC Rule 482 are an example of time-weighted returns. Time-weighted returns ignore the size and timing of investment cash flows and therefore provide a measure of manager or strategy performance, while IRR measures how a specific portfolio performed in absolute terms.

18. The CFA Institute is a global association of investment professionals. *See generally* CFA Institute Global Investment Performance Standards.

2022 Annual Conference

May 16 –18 | Washington, DC | Hybrid Event

Restricted Firm Obligations: What You Need to Know

Tuesday, May 17, 2022
9:45 a.m. – 10:45 a.m.

Join FINRA staff as they discuss Rule 4111 (Restricted Firm Obligations) which went into effect in January 2022. During the session, panelists review the new obligation and criteria for identification.

Moderator:

William St. Louis
Executive Vice President, National Cause & Financial Crimes Detection Programs
FINRA Member Supervision

Panelists:

Lance Burkett
Senior Director, Retail Risk Monitoring
FINRA Member Supervision

Kosha Dalal
Vice President and Associate General Counsel, Legal Policy
FINRA Office of General Counsel

Restricted Firm Obligations: What You Need to Know Panelists Bios:

Moderator:

Bill St. Louis is Senior Vice President and Firm Group Leader for FINRA member firms assigned to the Retail and Capital Markets firm groupings. In this capacity, he has responsibility for the Single Points of Accountability and Risk Monitoring Program teams for these firms, which includes the assessment of business conduct, financial, operational and trading risks. He and his team are also responsible for examination strategy for these firms, as well as coordination with Examination Program management on the execution of related examinations. He also oversees FINRA's High Risk Representative Program, and FINRA's Membership Application Program (MAP). Prior to his current role, Mr. St. Louis was the Regional Director for FINRA's Northeast region, District Director of FINRA's New York office, and held senior roles in FINRA's Enforcement Department including serving as the Regional Chief Counsel for FINRA's North Region. Mr. St. Louis earned an undergraduate degree from Baruch College and a law degree from New York University School of Law. Prior to law school he worked for several years in the Compliance Department of a NY-based broker-dealer.

Panelists:

Lance Burkett is Senior Director of Risk Monitoring in the FINRA Denver Office. He began his securities industry career in 1993 as a Securities Fraud Investigator for the State of Arizona Securities Division, working exclusively on fraud cases involving broker-dealers. Later, at a FINRA member firm, he was responsible for supervising Producing Branch Managers and Field Representatives as the Field Compliance Director. Throughout his tenure with FINRA, Mr. Burkett has held positions ranging from Compliance Examiner, District Director and now Senior Director - Risk Monitoring, responsible in overseeing the Risk Monitoring team and coordinating with the Examination Program Management on the execution of examinations of Member firms in the retail space. Mr. Burkett earned his Certified Regulatory and Compliance Professional™ designation through the FINRA Institute at Wharton and has developed content and presented at several FINRA Institute class offerings.

Kosha Dalal is Vice President and Associate General Counsel for Legal Policy with FINRA's Office of General Counsel. In this role, she provides legal guidance on various policy initiatives and rule changes/interpretations including, supervision, firms and brokers with a history of misconduct, branch office/OSJ, remote inspections, customer account statements, membership application rules, ACATs, payments to unregistered persons and corporate actions. She has been with FINRA's Office of General Counsel since 2000. Prior to coming to FINRA, she was an associate with the law firm of Venable in Baltimore, MD, Kalkines Zall in New York, NY and Skadden Arps in New York, NY. Ms. Dalal holds a BA in Political Science and Economics from Barnard University and a JD from Brooklyn Law School. Ms. Dalal also serves on FINRA's Diversity Leadership Council, which is tasked with recommending steps and initiatives to help FINRA develop and implement a robust diversity and inclusion strategy.

Restricted Firm Obligations: What You Need to Know

Panelists

- **Moderator**
  - William St. Louis, Executive Vice President, National Cause & Financial Crimes Detection Programs, FINRA Member Supervision
- **Panelists**
  - Lance Burkett, Senior Director, Retail Risk Monitoring, FINRA Member Supervision
  - Kosha Dalal, Vice President and Associate General Counsel, Legal Policy, FINRA Office of General Counsel

Restricted Firm Obligations: What You Need to Know
Tuesday, May 17, 2022
9:45 a.m. – 10:45 a.m.

Resources:

- FINRA *Information Notice 2/1/22, FINRA Announces Rule 4111 (Restricted Firm Obligations) Evaluation Date*

  www.finra.org/rules-guidance/notices/information-notice-020122

- FINRA *Regulatory Notice 21-34, FINRA Adopts Rules to Address Firms With a Significant History of Misconduct* (September 2021)

  www.finra.org/rules-guidance/notices/21-34

- FINRA *Regulatory Notice 19-17, FINRA Requests Comment on Proposed New Rule 4111 (Restricted Firm Obligations) Imposing Additional Obligations on Firms with a Significant History of Misconduct* (May 2019)

  www.finra.org/rules-guidance/notices/19-17

- FINRA Rule 4111 Frequently Asked Questions

  www.finra.org/rules-guidance/key-topics/protecting-investors-from-misconduct/faq

- FINRA Mapping of Disclosure Categories for FINRA Rule 4111

  www.finra.org/compliance-tools/mapping-disclosure-categories-finra-rule-4111

Attachment A

New and Amended Rule Text

New language is underlined; deletions are in brackets.

* * * * *

FINRA Rules

* * * * *

4000. FINANCIAL AND OPERATIONAL RULES

* * * * *

4111. Restricted Firm Obligations

(a) General

A member designated as a Restricted Firm shall be required, except as provided in paragraphs (e) and (f) of this Rule, to establish a Restricted Deposit Account and deposit in that account cash or qualified securities with an aggregate value that is not less than the member's Restricted Deposit Requirement, and shall be subject to such conditions or restrictions on the member's operations as determined by the Department to be necessary or appropriate for the protection of investors and in the public interest.

(b) Annual Calculation by FINRA of Preliminary Criteria for Identification

For each member, the Department will compute annually (on a calendar-year basis) the Preliminary Identification Metrics to determine if the member meets the Preliminary Criteria for Identification.

(c) Initial Department Evaluation and One-Time Staff Reduction

(1) Initial Department Evaluation

If the member is deemed to meet the Preliminary Criteria for Identification, the Department shall conduct an internal evaluation to determine whether (A) the member does not warrant further review under this Rule because the Department has information to conclude that the computation of the member's Preliminary Identification Metrics included disclosure events (and other conditions) that should not have been included because they are not consistent with the purpose of the Preliminary Criteria for Identification and are not reflective of a firm posing

a high degree of risk. The Department shall also consider whether the member has addressed the concerns signaled by the disclosure events or conditions or altered its business operations such that the Preliminary Criteria for Identification calculation no longer reflects the member's current risk profile, or (B) except as provided in paragraph (c)(2) of this Rule, the member should proceed to a Consultation.

(2) One-Time Staff Reduction

If the Department determines that the member meets the Preliminary Criteria for Identification and such member has met such criteria for the first time, such member may reduce its staffing levels to no longer meet the Preliminary Criteria for Identification within 30 business days after being informed by the Department. The member shall provide evidence of the staff reduction to the Department identifying the terminated individuals. Once the member has reduced staffing levels to no longer meet the Preliminary Criteria for Identification, it shall not rehire in any capacity a person terminated to accomplish the staff reduction for a period of one year.

(3) Close-Out Review

If the Department determines that the member no longer warrants further review in accordance with paragraph (c)(1)(A) or (c)(2) of this Rule, the Department shall close out the review of the member for such year.

(d) Consultation

(1) General

If the Department determines that the member meets the Preliminary Criteria for Identification and should proceed to a Consultation, the Department shall conduct the Consultation to allow the member to demonstrate why it does not meet the Preliminary Criteria for Identification and should not be designated as a Restricted Firm. If the member is designated as a Restricted Firm, the Department may require it to be subject to a Restricted Deposit Requirement or to such conditions or restrictions as the Department in its discretion shall deem necessary or appropriate for the protection of investors or in the public interest, or both. The member bears the burden of demonstrating that it should not be designated as a Restricted Firm and should not be subject to the maximum Restricted Deposit Requirement.

(A) A member may overcome the presumption that it should be designated as a Restricted Firm by clearly demonstrating that the Department's calculation that the member meets the Preliminary Criteria for Identification included events in the Disclosure Event and Expelled Firm Association Categories that should not have been included because for example, they are duplicative, involving the same customer and the same matter, or are not sales practice related; and

(B) A member may overcome the presumption that it should be subject to the maximum Restricted Deposit Requirement by clearly demonstrating to the Department that the member would face significant undue financial hardship if it were subject to the maximum Restricted Deposit Requirement and that a lesser deposit requirement would satisfy the objectives of this Rule and be consistent with the protection of investors and the public interest; or that conditions and restrictions on the operations and activities of the member and its associated persons would address the concerns indicated by the Preliminary Criteria for Identification and protect investors and the public interest.

(2) Scheduling Consultation

The Department shall provide a written letter to each member it determines should proceed to a Consultation or that will proceed to a Consultation pursuant to paragraph (f)(2) of this Rule at least seven days prior to the Consultation, of the date, time and place of the Consultation and shall coordinate with the member to schedule further meetings as necessary. A Consultation shall begin at the time scheduled, unless the Department, for good cause shown by the member, provides a written letter that postpones the commencement of the Consultation. Postponements shall not exceed 30 days unless the member establishes the reasons a longer postponement is necessary.

(3) Consultation Process

In conducting its evaluation of whether a member should be designated as a Restricted Firm and subject to a Restricted Deposit Requirement, the Department shall consider:

(A) information provided by the member during any meetings as part of the Consultation;

(B) relevant information or documents, if any, submitted by the member, in the manner and form prescribed by the Department, as shall be necessary or appropriate for the Department to review the computation of the Preliminary Criteria for Identification;

(C) a plan, if any, submitted by the member, in the manner and form prescribed by the Department, proposing in detail the specific conditions or restrictions that the member seeks to have the Department consider;

(D) such other information or documents as the Department may reasonably request in its discretion from the member related to the evaluation; and

(E) any other information the Department deems necessary or appropriate to evaluate the matter.

(e) Department Decision and Notice

(1) Department Decision

Following the Consultation, but no later than 30 days from the date of the latest letter provided to the member under paragraph (d)(2) of this Rule, the Department shall render a Department Decision as follows:

(A) If the Department determines that the member has rebutted the presumption set forth in paragraph (d)(1)(A) of this Rule that it should be designated as a Restricted Firm, the Department's decision shall state that the firm shall not be designated as a Restricted Firm.

(B) If the Department determines that the member has failed to rebut the presumption set forth in paragraphs (d)(1)(A) and (d)(1)(B) of this Rule that it should be designated as a Restricted Firm that shall be subject to the maximum Restricted Deposit Requirement, the Department's decision shall designate the member as a Restricted Firm and require the member to: (i) promptly establish a Restricted Deposit Account and deposit in that account the maximum Restricted Deposit Requirement; and (ii) implement and maintain specified conditions or restrictions, as the Department deems necessary or appropriate, on the operations and activities of the member and its associated persons to address the concerns indicated by the Preliminary Criteria for Identification and protect investors and the public interest.

(C) If the Department determines that the member has failed to rebut the presumption in paragraph (d)(1)(A) of this Rule that it should be designated as a Restricted Firm but that it has rebutted the presumption in paragraph (d)(1)(B) of this Rule that it shall be subject to the maximum Restricted Deposit Requirement, the Department shall designate the member as a Restricted Firm and shall: (i) impose no Restricted Deposit Requirement on the member or require the member to promptly establish a Restricted Deposit Account and deposit in that account a Restricted Deposit Requirement in such dollar amount less than the maximum Restricted Deposit Requirement as the Department deems necessary or appropriate; and (ii) require the member to implement and maintain specified conditions or restrictions, as the Department deems necessary or appropriate, on the operations and activities of the member and its associated persons to address the concerns indicated by the Preliminary Criteria for Identification and protect investors and the public interest.

(2) Notice of Department Decision, No Stays

No later than 30 days following the latest letter provided to the member under paragraph (d)(2) of this Rule, the Department shall issue a notice of the Department's decision pursuant to Rule 9561(a) that states the obligations to be imposed on the member, if any, under this Rule 4111 and the ability of the member under Rule 9561 to request a hearing with the Office of Hearing Officers. A timely request for a hearing shall not stay the effectiveness of the notice issued under Rule 9561(a), except that for a notice under Rule 9561(a) a member subject to a Restricted Deposit Requirement shall be required to deposit in a Restricted Deposit Account the lesser of 25 percent of its Restricted Deposit Requirement or 25 percent of its average excess net capital during the prior calendar year, until the Office of Hearing Officers or the NAC issues a written decision under Rule 9559; provided, however, that a member that has been re-designated as a Restricted Firm as set forth in paragraph (f)(2) of this Rule and is already subject to a previously imposed Restricted Deposit Requirement shall be required to keep in the Restricted Deposit Account the assets then on deposit therein until the Office of Hearing Officers or NAC issues a written decision under Rule 9559.

(f) Continuation or Termination of Restricted Firm Obligations

(1) Currently Designated Restricted Firms

A member or Former Member that is currently designated as a Restricted Firm subject to the requirements of this Rule shall not be permitted to withdraw all or any portion of its Restricted Deposit Requirement, or seek to terminate or modify any deposit requirement, conditions, or restrictions that have been imposed pursuant to this Rule, without the prior written consent of the Department. There shall be a presumption that the Department shall deny an application by a member or Former Member that is currently designated as a Restricted Firm to withdraw all or any portion of its Restricted Deposit Requirement. An application under this paragraph for a withdrawal from a Restricted Deposit Requirement shall comply with the content requirements in paragraph (f)(3)(A)(i) through (iv) of this Rule.

(2) Re-Designation as a Restricted Firm

Where a member has been designated as a Restricted Firm in one year and is determined to meet the Preliminary Criteria for Identification the following year in accordance with paragraph (b) of this Rule, the Department shall provide a written letter to the member stating that it shall be re-designated as a Restricted Firm, and that the obligations previously imposed on the member in accordance with this Rule shall remain effective and unchanged, unless either the member or the Department requests a Consultation in writing within seven days of the date of the letter, in which case the obligations previously imposed shall remain effective and unchanged unless and until the Department modifies or terminates them after the Consultation. If a Consultation is conducted, there shall be a presumption that the Restricted Deposit Requirement and conditions or restrictions, if any, previously imposed on the member shall remain effective and unchanged absent a showing by the party seeking changes that the previously imposed obligations are no longer necessary or appropriate for the protection of investors or in the public interest. If a Consultation is not timely requested, the member shall be subject to paragraph (f)(1) of this Rule. When FINRA re-designates a member as a Restricted Firm and the member is subject to a Restricted Deposit Requirement, the member shall promptly after such re-designation (or, in the case where a hearing is requested pursuant to Rule 9561, promptly after the Office of Hearing Officers or the NAC issues a written decision under Rule 9559) deposit additional cash or qualified securities in the member's Restricted Deposit Account to the extent necessary to

cause the aggregate value of the cash and qualified securities in the member's Restricted Deposit Account to be not less than its re-designated Restricted Deposit Requirement.

(3) Previously Designated Restricted Firms

(A) A member or Former Member that is a Restricted Firm in one year, but does not meet the Preliminary Criteria for Identification or is not designated as a Restricted Firm the following year(s), shall no longer be subject to any deposit requirement, conditions, or restrictions previously imposed on it under this Rule; provided, however, the member or Former Member shall not be permitted to withdraw any portion of its Restricted Deposit Requirement without submitting an application and obtaining the prior written consent of the Department. Such application shall:

(i) be made in such form and manner as FINRA may prescribe;

(ii) be accompanied by a copy of a current account statement for the member or Former Member's Restricted Deposit Account;

(iii) include a certification by the member's or Former Member's chief executive officer (or equivalent officer) stating the member's or Former Member's Restricted Deposit Requirement; the value of the cash or qualified securities on deposit in the member's or Former Member's Restricted Deposit Account; the value of cash or qualified securities on deposit in the member's or Former Member's Restricted Deposit Account that the member or Former Member is seeking the Department's consent to withdraw; and

(iv) include evidence that there are no "Covered Pending Arbitration Claims," unpaid arbitration awards or unpaid settlements relating to arbitrations outstanding against the member, the member's Associated Persons or the Former Member, or if there are any "Covered Pending Arbitration Claims," unpaid arbitration awards or unpaid settlements relating to arbitrations outstanding, provide a detailed description of such.

(B) After such review and investigation as it considers necessary or appropriate, the Department shall determine whether to authorize a withdrawal, in part or whole, of cash or qualified securities from the member's or Former Member's Restricted Deposit Account. There shall be presumptions

that the Department shall: (i) approve an application for withdrawal if the member, the member's Associated Persons, or the Former Member have no "Covered Pending Arbitration Claims," unpaid arbitration awards or unpaid settlements relating to arbitrations outstanding; and (ii) (a) deny an application for withdrawal if the member, the member's Associated Persons who are owners or control persons, or the Former Member have any "Covered Pending Arbitration Claims," unpaid arbitration awards or unpaid settlements relating to arbitrations outstanding, or if the member's Associated Persons have any "Covered Pending Arbitration Claims," unpaid arbitration awards or unpaid settlements relating to arbitrations outstanding that involved conduct or alleged conduct that occurred while associated with the member; but (b) approve an application by a Former Member for withdrawal if the Former Member commits in the manner specified by the Department to use the amount it seeks to withdraw from its Restricted Deposit to pay the Former Member's specified unpaid arbitration awards or unpaid settlements relating to arbitrations outstanding. Within 30 days from the date the application is received by the Department, the Department shall issue a notice of the Department's decision pursuant to Rule 9561(a).

(g) Books and Records

Each member shall maintain records evidencing the member's compliance with this Rule and any Restricted Deposit Requirement or conditions or restrictions imposed in accordance with this Rule, including without limitation, records relating to the calculation of the Preliminary Criteria for Identification, Consultation, the Restricted Deposit Account, conditions or restrictions imposed, and agreements with bank(s) or clearing firm(s), for a period of six years from the date the member is no longer subject to the requirements of this Rule. In addition, a firm that is subject to a Restricted Deposit Requirement shall provide to the Department, upon its request, records, agreements and account statements that demonstrate the firm's compliance with the Restricted Deposit Requirement.

(h) Notice of Failure to Comply

FINRA may issue a notice pursuant to Rule 9561(b) directing a member that is not in compliance with the Restricted Deposit Requirement or the conditions or restrictions imposed by this Rule to suspend all or a portion of its business.

(i) Definitions

For purposes of this Rule, the following terms shall have the following meanings:

(1) The term "Consultation" means one or more meetings or consultations between the Department and a member that meets the Preliminary Criteria for Identification.

(2) The term "Covered Pending Arbitration Claim," for purposes of this Rule 4111, means an investment-related, consumer initiated claim filed against the member or its Associated Persons in any arbitration forum that is unresolved; and whose claim amount (individually or, if there is more than one claim, in the aggregate) exceeds the member's excess net capital. For purposes of this definition, the claim amount includes claimed compensatory loss amounts only, not requests for pain and suffering, punitive damages or attorney's fees, and shall be the maximum amount for which the member or Associated Person, as applicable, is potentially liable regardless of whether the claim was brought against additional persons or the Associated Person reasonably expects to be indemnified, share liability or otherwise lawfully avoid being held responsible for all or part of such maximum amount.

(3) The term "Department" means FINRA's Department of Member Regulation.

(4) The term "Disclosure Event and Expelled Firm Association Categories" means the following categories of disclosure events and other information:

(A) "Registered Person Adjudicated Events" means any one of the following events that are reportable on the registered person's Uniform Registration Forms:

(i) a final investment-related, consumer-initiated customer arbitration award or civil judgment against the registered person in which the registered person was a named party or was a "subject of" the customer arbitration award or civil judgment;

(ii) a final investment-related, consumer-initiated customer arbitration settlement, civil litigation settlement or a settlement prior to a customer arbitration or civil litigation for a dollar amount at or above $15,000 in which the registered person was a named party or was a "subject of" the customer arbitration settlement, civil litigation settlement or a settlement prior to a customer arbitration or civil litigation;

(iii) a final investment-related civil judicial matter that resulted in a finding, sanction or order;

(iv) a final regulatory action that resulted in a finding, sanction or order, and was brought by the SEC or Commodity Futures Trading Commission (CFTC), other federal regulatory agency, a state regulatory agency, a foreign financial regulatory authority, or a self-regulatory organization; or

(v) a criminal matter in which the registered person was convicted of or pled guilty or nolo contendere (no contest) in a domestic, foreign, or military court to any felony or any reportable misdemeanor.

(B) "Registered Person Pending Events" means any one of the following events associated with the registered person that are reportable on the registered person's Uniform Registration Forms:

(i) a pending investment-related civil judicial matter;

(ii) a pending investigation by a regulatory authority;

(iii) a pending regulatory action that was brought by the SEC or CFTC, other federal regulatory agency, a state regulatory agency, a foreign financial regulatory authority, or a self-regulatory organization; or

(iv) a pending criminal charge associated with any felony or any reportable misdemeanor.

(C) "Registered Person Termination and Internal Review Events" means any one of the following events associated with the registered person at a previous member that are reportable on the registered person's Uniform Registration Forms:

(i) a termination in which the registered person voluntarily resigned, was discharged or was permitted to resign from a previous member after allegations; or

(ii) a pending or closed internal review by a previous member.

(D) "Member Firm Adjudicated Events" means any one of the following events that are reportable on the member's Uniform Registration Forms, or are based on customer arbitrations filed with FINRA's dispute resolution forum:

(i) a final investment-related, consumer-initiated customer arbitration award in which the member was a named party;

(ii) a final investment-related civil judicial matter that resulted in a finding, sanction or order;

(iii) a final regulatory action that resulted in a finding, sanction or order, and was brought by the SEC or CFTC, other federal regulatory agency, a state regulatory agency, a foreign financial regulatory authority, or a self-regulatory organization; or

(iv) a criminal matter in which the member was convicted of or pled guilty or nolo contendere (no contest) in a domestic, foreign, or military court to any felony or any reportable misdemeanor.

(E) "Member Firm Pending Events" means any one of the following events that are reportable on the member's Uniform Registration Forms:

(i) a pending investment-related civil judicial matter;

(ii) a pending regulatory action that was brought by the SEC or CFTC, other federal regulatory agency, a state regulatory agency, a foreign financial regulatory authority, or a self-regulatory organization; or

(iii) a pending criminal charge associated with any felony or any reportable misdemeanor.

(F) "Registered Persons Associated with Previously Expelled Firms" means any Registered Person In-Scope who was registered for at least one year with a previously expelled firm and whose registration with the previously expelled firm terminated during the Evaluation Period.

(5) The term "Evaluation Date" means the date, each calendar year, as of which the Department calculates the Preliminary Identification Metrics to determine if the member meets the Preliminary Criteria for Identification.

(6) The term "Evaluation Period" means the prior five years from the Evaluation Date, provided that for the Registered Person Pending Events and Member Firm Pending Events categories and pending internal reviews in the Registered Person Termination and Internal Review Events category, it would correspond to the Evaluation Date (and include all events that are pending as of the Evaluation Date).

(7) The term "Former Member" means an entity that has withdrawn or resigned its FINRA membership, or that has had its membership cancelled or revoked.

(8) The term "qualified security" has the meaning given it in SEA Rule 15c3-3(a)(6).

(9) The term "Preliminary Criteria for Identification" means meeting the following conditions:

(A) Two or more of the member's Preliminary Identification Metrics are equal to or more than the corresponding Preliminary Identification Metrics Thresholds, and at least one of these metrics is among the following metrics:

(i) Registered Person Adjudicated Event Metric;

(ii) Member Firm Adjudicated Event Metric; and

(iii) Expelled Firm Association Metric; and

(B) The member has two or more Registered Person and Member Firm Events during the Evaluation Period.

(10) The term "Preliminary Identification Metrics" means the following six metrics that are based on the number of disclosure events (defined above) per Registered Persons In-Scope or percent of Registered Persons In-Scope associated with previously expelled firms:

(A) "Registered Person Adjudicated Event Metric" would be computed as the sum of Registered Person Adjudicated Events that reached a resolution during the Evaluation Period, across all Registered Persons In-Scope and divided by the number of Registered Persons In-Scope.

(B) "Registered Person Pending Event Metric" would be computed as the sum of Registered Person Pending Events as of the Evaluation Date, across all Registered Persons In-Scope and divided by the number of Registered Persons In-Scope.

(C) "Registered Person Termination and Internal Review Event Metric" would be computed as the sum of Registered Person Termination and Internal Review Events that reached a resolution during the Evaluation Period and pending internal reviews by a previous member as of the Evaluation Date, across all Registered Persons In-Scope and divided by the number of Registered Persons In-Scope.

(D) "Member Firm Adjudicated Event Metric" would be computed as the sum of Member Firm Adjudicated Events that reached a resolution during the Evaluation Period, divided by the number of Registered Persons In-Scope.

(E) "Member Firm Pending Event Metric" would be computed as the sum of Member Firm Pending Events as of the Evaluation Date, divided by the number of Registered Persons In-Scope.

(F) "Expelled Firm Association Metric" would be computed as the sum of Registered Persons Associated with Previously Expelled Firms, divided by the number of Registered Persons In-Scope.

(11) The term "Preliminary Identification Metrics Thresholds" means the following thresholds corresponding to each of the six Preliminary Identification Metrics.

Firm Size Category	Number of Registered Persons In-Scope in Firm Size Category	Preliminary Identification Metrics Thresholds					
		Thresholds for Registered Person Event Metrics:			Thresholds for Member Firm Event Metrics:		Threshold for Expelled Firm Association Metric:
		Registered Person Adjudicated Event Metric	Registered Person Pending Event Metric	Registered Person Termination and Internal Review Event Metric	Member Firm Adjudicated Event Metric	Member Firm Pending Event Metric	Expelled Firm Association Metric
		(1)	(2)	(3)	(4)	(5)	(6)
1	1-4	0.50	0.20	0.10	0.75	0.25	0.30
2	5-9	0.30	0.20	0.10	0.30	0.10	0.25
3	10-19	0.20	0.10	0.10	0.30	0.05	0.20
4	20-50	0.20	0.10	0.10	0.20	0.02	0.15
5	51-150	0.20	0.05	0.10	0.15	0.01	0.03
6	151-499	0.15	0.05	0.10	0.10	0.01	0.01
7	500+	0.10	0.05	0.10	0.05	0.01	0.01

(12) The term "Registered Person and Member Firm Events" means the sum of the following categories of defined events during the Evaluation Period:

(A) Registered Person Adjudicated Events;

(B) Registered Person Pending Events;

(C) Registered Person Termination and Internal Review Events;

(D) Member Firm Adjudicated Events; and

(E) Member Firm Pending Events.

(13) The term "Registered Persons In-Scope" means all persons registered with the firm for one or more days within the one year prior to the Evaluation Date.

(14) The term "Restricted Deposit Account" means an account in the name of the member:

(A) at a bank (as defined in Section 3(a)(6) of the Exchange Act) or the member's clearing firm;

(B) subject to an agreement in which the bank or the member's clearing firm, as applicable, agrees:

(i) not to permit withdrawals (other than withdrawals of interest or the withdrawal of qualified securities or cash after and on the same day as the deposit of cash or qualified securities of equal value) from the Restricted Deposit Account without the prior written consent of FINRA;

(ii) to keep the account separate from any other accounts maintained by the member with the bank or clearing firm;

(iii) that the cash or securities on deposit in the account will at no time be used directly or indirectly as security for a loan to the member by the bank or clearing firm and will not be subject to any set-off, right, charge, security interest, lien, or claim of any kind in favor of the bank, clearing firm or any person claiming through the bank or clearing firm;

(iv) that if the member becomes a Former Member, the assets deposited in the Restricted Deposit Account to satisfy the Restricted Deposit Requirement shall be kept in the Restricted Deposit Account, and the bank or clearing firm will not permit withdrawals from the Restricted Deposit Account without the prior written consent of FINRA as set forth in paragraphs (f)(1) and (f)(3) of this Rule; and

(v) that FINRA is a third-party beneficiary to such agreement and that such agreement may not be amended without the prior written consent of FINRA; and

(C) not subject to any right, charge, security interest, lien or claim of any kind granted by the member.

(15) The term "Restricted Deposit Requirement" means one of the following amounts:

(A) the specific maximum Restricted Deposit Requirement for a member, determined by the Department taking into consideration the nature of the firm's operations and activities, revenues, commissions, assets, liabilities, expenses, net capital, the number of offices and registered persons, the nature of the disclosure events counted in the numeric thresholds, insurance coverage for customer arbitration awards or settlements, concerns raised during FINRA exams, and the amount of any of the firm's or its Associated Persons' Covered Pending Arbitration Claims, unpaid arbitration awards or unpaid settlements related to arbitrations. Based on a review of these factors, the Department would determine a maximum Restricted Deposit Requirement for the member that would be consistent with the objectives of this Rule, but would not significantly undermine the continued financial stability and operational capability of the firm as an ongoing enterprise over the next 12 months; or

(B) the amount, adjusted after the Consultation, determined by the Department; and

(C) with respect to a Former Member, the Restricted Deposit Requirement last calculated pursuant to paragraph (i)(15)(A) or (15)(B) of this Rule when the firm was a member.

(16) The term "Restricted Firm" means each member that is designated as such in accordance with paragraphs (e)(1)(B) and (e)(1)(C) of this Rule.

(17) The term "Uniform Registration Forms" means the Forms BD, U4, U5 and U6, as applicable.

• • • Supplementary Material: ----------

.01 Net Capital Treatment of the Deposits in the Restricted Deposit Account. Because of the restrictions on withdrawals from a Restricted Deposit Account, deposits in such an account cannot be readily converted into cash and therefore shall be deducted in determining the member's net capital under SEA Rule 15c3-1 and FINRA Rule 4110.

.02 Compliance with Rule 1017. Nothing in this Rule shall be construed as altering in any manner a member's obligations under Rule 1017.

.03 Examples of Conditions and Restrictions. For purposes of this Rule, the conditions or restrictions that the Department may impose include, but are not limited to, the following:

(a) limitations on business expansions, mergers, consolidations or changes in control;

(b) filing all advertising with FINRA's Department of Advertising Regulation;

(c) imposing requirements on establishing and supervising offices;

(d) requiring a compliance audit by a qualified, independent third party;

(e) limiting business lines or product types offered;

(f) limiting the opening of new customer accounts;

(g) limiting approvals of registered persons entering into borrowing or lending arrangements with their customers;

(h) requiring the member to impose specific conditions or limitations on, or to prohibit, registered persons' outside business activities of which the member has received notice pursuant to Rule 3270; and

(i) requiring the member to prohibit or, as part of its supervision of approved private securities transactions for compensation under Rule 3280 or otherwise, impose specific conditions on associated persons' participation in private securities transactions of which the member has received notice pursuant to Rule 3280.

* * * * *

9500. OTHER PROCEEDINGS

* * * * *

9550. Expedited Proceedings

* * * * *

9559. Hearing Procedures for Expedited Proceedings Under the Rule 9550 Series

(a) No Change.

(b) Computation of Time

Rule 9138 shall govern the computation of time in proceedings brought under the Rule 9550 Series, except that intermediate Saturdays, Sundays and Federal holidays shall be included in the computation in proceedings brought under Rules 9556 through 9558 and 9561, unless otherwise specified.

(c) Stays

(1) Unless the Chief Hearing Officer or the Hearing Officer assigned to the matter orders otherwise for good cause shown, a timely request for a hearing shall stay the effectiveness of a notice issued under Rules 9551 through 9556 and 9561(b), except that: (A) the effectiveness of a notice of a limitation or prohibition on access to services offered by FINRA or a member thereof under Rule 9555 with respect to services to which the member or person does not have access shall not be stayed by a request for a hearing; and (B) this paragraph has no applicability to a petition instituting an expedited proceeding under Rule 9556(h).

(2) A timely request for a hearing shall stay the effectiveness of a notice issued under Rule 9557 for 10[ten] business days after service of the notice or until the Office of Hearing Officers issues a written order under Rule 9559(o)(4)(A) (whichever period is less), unless FINRA's Chief Executive Officer (or such other executive officer as the Chief Executive Officer may designate) determines that a notice under Rule 9557 shall not be stayed. Where a notice under Rule 9557 is stayed by a request for a hearing, such stay shall remain in effect only for 10[ten] business days after service of the notice or until the Office of Hearing Officers issues a written order under Rule 9559(o)(4)(A) (whichever period is less) and shall not be extended.

(3) No Change.

(4) A timely request for a hearing shall not stay the effectiveness of a notice issued under Rule 9561(a).

(d) Appointment and Authority of Hearing Officer and[/or] Hearing Panel

(1) For proceedings initiated under Rules 9553, 9554, [and] 9556(h) and 9561, the Chief Hearing Officer shall appoint a Hearing Officer to preside over and act as the sole adjudicator for the matter.

(2) through (6) No Change.

(e) Consolidation or Severance of Proceedings

Rule 9214 shall govern the consolidation or severance of proceedings, except that, where one of the notices that are the subject of consolidation under this Rule requires that a hearing be held before a Hearing Panel, the hearing of the consolidated matters shall be held before a Hearing Panel. Where two consolidated matters contain different timelines under this Rule, the Chief Hearing Officer or Hearing Officer assigned to the matter has discretion to determine which timeline is appropriate under the facts and circumstances of the case. Where one of the consolidated matters includes an action brought under a Rule that does not permit a stay of the effectiveness of the notice or where FINRA's Chief Executive Officer (or such other executive officer as the Chief Executive Officer may designate), in the case of Rule 9557, or Hearing Officer, in the case of Rule 9558(d), determines that a request for a hearing shall not stay the effectiveness of the notice, the limitation, prohibition, condition, requirement, restriction, obligation or suspension specified in the notice, or the partial deposit requirement specified in Rule 9561(a)(4), shall not be stayed pending resolution of the case. Where one of the consolidated matters includes an action brought under Rule 9557 that is stayed for up to 10[ten] business days, the requirement [and/]or restriction specified in the notice shall not be further stayed.

(f) Time of Hearing

(1) No Change.

(2) A hearing shall be held within 10[ten] days after a respondent is served a petition seeking an expedited proceeding issued under Rules 9556(h).

(3) A hearing shall be held within 14 days after a respondent subject to a notice issued under Rules 9556 (except Rule 9556(h)), [and] 9558 or 9561(b) files a written request for a hearing with the Office of Hearing Officers.

(4) No Change.

(5) A hearing shall be held within 30 days after a respondent subject to a notice issued under Rule 9561(a) files a written request for a hearing with the Office of Hearing Officers.

([5]6) The timelines established by paragraphs (f)(1) through (f)(5[4]) of this Rule confer no substantive rights on the parties.

(g) Notice of Hearing

The Hearing Officer shall issue a notice stating the date, time, and place of the hearing as follows:

(1) through (2) No Change.

(3) At least seven days prior to the hearing in the case of an action brought pursuant to Rules 9556 (except Rule 9556(h)), [and] 9558 or 9561(b); and

(4) At least 21 days prior to the hearing in the case of an action brought pursuant to Rules 9551 through 9555 or 9561(a).

(h) Transmission of Documents

(1) Not less than two business days before the hearing in an action brought under Rule 9557, not less than six days before the hearing in an action brought under Rule 9556(h), not less than seven days before the hearing in an action brought under Rules 9556 (except Rule 9556(h)), [and] 9558 or 9561(b), and not less than 14 days before the hearing in an action brought under Rules 9551 through 9555 or 9561(a), FINRA staff shall provide to the respondent who requested the hearing or the respondent who has received a petition pursuant to Rule 9556(h), by facsimile, email, overnight courier or personal delivery, all documents that were considered in issuing the notice unless a document meets the criteria of Rule 9251(b)(1)(A), (B), (C) or (b)(2). Documents served by facsimile or email shall also be served by either overnight courier or personal delivery. A document that meets the criteria in this paragraph shall not constitute part of the record, but shall be retained by FINRA until the date upon which FINRA serves a final decision or, if applicable, upon the conclusion of any review by the SEC or the federal courts.

(2) Not less than two business days before the hearing in an action brought under Rule 9557, not less than three days before the hearing in an action brought under Rules 9556, [and] 9558 or 9561(b), and not less than seven days before the hearing in an action brought under Rules 9551 through 9555 or 9561(a), the parties shall exchange proposed exhibit and witness lists. The exhibit and witness lists shall be served by facsimile, email, overnight courier or personal delivery. Documents served by facsimile or email shall also be served by either overnight courier or personal delivery.

(i) through (m) No Change.

(n) Sanctions, Requirements, Costs and Remands

(1) In any action brought under the Rule 9550 Series, other than an action brought under Rule 9556(h), [or] Rule 9557 or Rule 9561, the Hearing Officer or, if applicable, the Hearing Panel may approve, modify or withdraw any and all sanctions, requirements, restrictions or limitations imposed by the notice and, pursuant to Rule 8310(a), may also impose any other fitting sanction.

(2) No Change.

(3) In an action brought under Rule 9557, the Hearing Panel shall approve or withdraw the requirements [and/]or restrictions imposed by the notice. If the Hearing Panel approves the requirements [and/]or restrictions and finds that the respondent has not complied with all of them, the Hearing Panel shall impose an immediate suspension on the respondent that shall remain in effect unless FINRA staff issues a letter of withdrawal of all requirements [and/]or restrictions pursuant to Rule 9557(g)(2).

(4) through (5) No Change.

(6) In any action brought under Rule 9561(a), the Hearing Officer may approve or withdraw any and all of the Rule 4111 Requirements, or remand the matter to the department that issued the notice for further consideration of specified matters, but may not modify any of the Rule 4111 Requirements imposed by the notice or impose any other requirements, obligations or restrictions available under Rule 4111. In any action brought under Rule 9561(b), the Hearing Officer may approve or withdraw the suspension or cancellation of membership, and may impose any other fitting sanction.

(o) Timing of Decision

(1) Proceedings initiated under Rules 9553, [and] 9554 and 9561

Within 60 days of the date of the close of the hearing, the Hearing Officer shall prepare a proposed written decision and provide it to the National Adjudicatory Council's Review Subcommittee.

(2) through (4) No Change.

(5) If not timely called for review by the National Adjudicatory Council's Review Subcommittee pursuant to paragraph (q) of this Rule, the Hearing Officer's or, if applicable, the Hearing Panel's written decision shall constitute final FINRA action. For decisions issued under Rules 9551 through 9556, [and] 9558 or 9561, the Office of Hearing Officers shall promptly serve the decision of the Hearing Officer or, if applicable, the Hearing Panel on the Parties and provide a copy to each FINRA member with which the respondent is associated.

(6) No Change.

(p) Contents of Decision

The decision, which for purposes of Rule 9557 means the written decision issued under paragraph (o)(4)(B) of this Rule, shall include:

(1) through (5) No Change.

(6) a statement describing any sanction, requirement, obligation, restriction or limitation imposed, the reasons therefore, and the date upon which such sanction, requirement, obligation, restriction or limitation shall become effective, if they are not already effective.

(q) through (r) No Change.

9561. Procedures for Regulating Activities Under Rule 4111

(a) Notices Under Rule 4111

(1) Notice of Requirements or Restrictions

FINRA's Department of Member Regulation ("Department") shall issue a notice of its determination under Rule 4111 that a firm is a Restricted Firm and the requirements, conditions or restrictions to which the Restricted Firm is subject (hereinafter, collectively referred to as the "Rule 4111 Requirements").

(2) Service of Notice

FINRA staff shall serve the member subject to a notice issued under this Rule (or upon counsel representing the member, or other person authorized to represent others under Rule 9141, when counsel or other person authorized to represent others under Rule 9141 agrees to accept service for the member) by facsimile, email, overnight courier or personal delivery. Papers served on a member, counsel for such member, or other person authorized to represent others under Rule 9141 by overnight courier or personal delivery shall conform to paragraphs (a)(1) and (3) and, with respect to a member, (b)(2) of Rule 9134. Papers served on a member by facsimile shall be sent to the member's facsimile number listed in the FINRA Contact System submitted to FINRA pursuant to Article 4, Section III of the FINRA By-Laws, except that, if FINRA staff has actual knowledge that a member's FINRA Contact System facsimile number is out of date, duplicate copies shall be sent to the member by overnight courier or personal delivery in conformity with paragraphs (a)(1) and (3) and (b)(2) of Rule 9134. Papers served on a member by email shall be sent to the member's email address listed in the FINRA Contact System submitted to FINRA pursuant to Article 4, Section III of the FINRA By-Laws and shall also be served by either overnight courier or personal delivery in conformity with paragraphs (a)(1) and (3) and (b)(2) of Rule 9134. Papers served on counsel for a member, or other person authorized to represent others under Rule 9141 by facsimile or email shall be sent to the facsimile number or email address that counsel or other person authorized to represent others under Rule 9141 provides and shall also be served by either overnight courier or personal delivery in conformity with paragraphs (a)(1) and (3) of Rule 9134. Service is complete upon sending the notice by facsimile or email, sending the notice by overnight courier or delivering it in person, except that, where duplicate service is required, service is complete upon sending the duplicate service.

(3) Contents of Notice

A notice issued under this Rule shall include the Department's determinations under Rule 4111 and state the specific grounds and include the factual basis for the FINRA action. The notice shall state when the FINRA action will take effect. The notice shall state that the respondent may file a written request for a hearing with the Office of Hearing Officers pursuant to Rule 9559. The notice also shall inform the respondent of the applicable deadline for filing a request for a hearing and shall state that a request for a hearing must set forth with specificity the basis for

eliminating any Rule 4111 Requirements. In addition, the notice shall explain that, pursuant to Rule 9559(n), a Hearing Officer may approve or withdraw any and all of the Rule 4111 Requirements, or remand the matter to the Department that issued the notice for further consideration of specified matters, but may not modify any of the Rule 4111 Requirements imposed by the notice or impose any other obligations or restrictions available under Rule 4111.

(4) Effectiveness of the Rule 4111 Requirements

The Rule 4111 Requirements imposed by a notice issued and served under paragraph (a) of this Rule are immediately effective; provided, however, that when a firm requests review of a Department determination under Rule 4111 that imposes a deposit requirement on the firm for the first time, the firm shall be required to deposit only 25 percent of its restricted deposit requirement or 25 percent of its average excess net capital over the prior year, whichever is less, while the hearing is pending. The Rule 4111 Requirements, and the partial deposit requirement required by Rule 4111 and this paragraph, shall remain in effect while the hearing is pending.

(5) Request for Hearing

A member served with a notice under paragraph (a) of this Rule may file with the Office of Hearing Officers a written request for a hearing pursuant to Rule 9559. A request for a hearing shall be made within seven days after service of the notice issued under this Rule. A request for a hearing must set forth with specificity the basis for eliminating any Rule 4111 Requirements.

(6) Failure to Request Hearing

If a member does not timely request a hearing, the notice under paragraph (a) of this Rule shall constitute final FINRA action.

(b) Notice for Failure to Comply with the Rule 4111 Requirements

(1) Notice of Suspension or Cancellation

If a member fails to comply with any Rule 4111 Requirements imposed under this Rule, the Department, after receiving authorization from FINRA's Chief Executive Officer or such other executive officer as the Chief Executive Officer may designate, may issue a suspension or cancellation notice to such member stating that the failure to comply with the Rule 4111 Requirements within seven days of service of the notice will result in a suspension or cancellation of membership.

(2) Service of Notice

FINRA staff shall serve the member subject to a notice issued under this paragraph (b) in accordance with the service provisions in paragraph (a)(2) of this Rule.

(3) Contents of Notice

The notice shall explicitly identify the Rule 4111 Requirements with which the firm is alleged to have not complied and shall contain a statement of facts specifying the alleged failure. The notice shall state when the suspension will take effect and explain what the respondent must do to avoid such suspension. The notice shall state that the respondent may file a written request for a hearing with the Office of Hearing Officers pursuant to Rule 9559. The notice also shall inform the respondent of the applicable deadline for filing a request for a hearing and shall state that a request for a hearing must set forth with specificity any and all defenses to the FINRA action. In addition, the notice shall explain that, pursuant to Rules 8310(a) and 9559(n), a Hearing Officer may approve or withdraw the suspension or cancellation of membership, and may impose any other fitting sanction.

(4) Effective Date of Suspension or Cancellation

The suspension or cancellation referenced in a notice issued and served under paragraphs (b)(1) and (b)(2) of this Rule shall become effective seven days after service of the notice, unless stayed by a request for hearing pursuant to Rule 9559.

(5) Request for a Hearing

A member served with a notice under paragraphs (b)(1) and (b)(2) of this Rule may file with the Office of Hearing Officers a written request for a hearing pursuant to Rule 9559. A request for a hearing shall be made before the effective date of the notice, as indicated in paragraph (b)(4) of this Rule. A request for a hearing must set forth with specificity any and all defenses to the FINRA action.

(6) Failure to Request Hearing

If a member does not timely request a hearing, the suspension or cancellation specified in the notice shall become effective seven days after the service of the notice and the notice shall constitute final FINRA action.

(7) Request for Termination of the Suspension

A member subject to a suspension imposed after the process described in paragraphs (b)(1) through (6) of this Rule may file a written request for termination of the suspension on the ground of full compliance with the notice or decision. Such request shall be filed with the head of the Department. The head of the Department may grant relief for good cause shown.

• • • Supplementary Material: ----------

.01 Application to Former Members Under Rule 4111. For purposes of this Rule, the term member also shall include a "Former Member" as defined in Rule 4111(i) as applicable.

* * * * *

Capital Acquisition Broker Rules

* * * * *

400. FINANCIAL AND OPERATIONAL RULES

* * * * *

412. Restricted Firm Obligations

All capital acquisition brokers are subject to FINRA Rule 4111.

* * * * *

Funding Portal Rules

* * * * *

900. Code of Procedure.

(a) Application of FINRA Rule 9000 Series (Code of Procedure) to Funding Portals

Except for the FINRA Rule 9520 Series, FINRA Rule 9557, FINRA Rule 9561, and the FINRA Rule 9700 Series, all funding portal members shall be subject to the FINRA Rule 9000 Series, unless the context requires otherwise, provided, however, that:

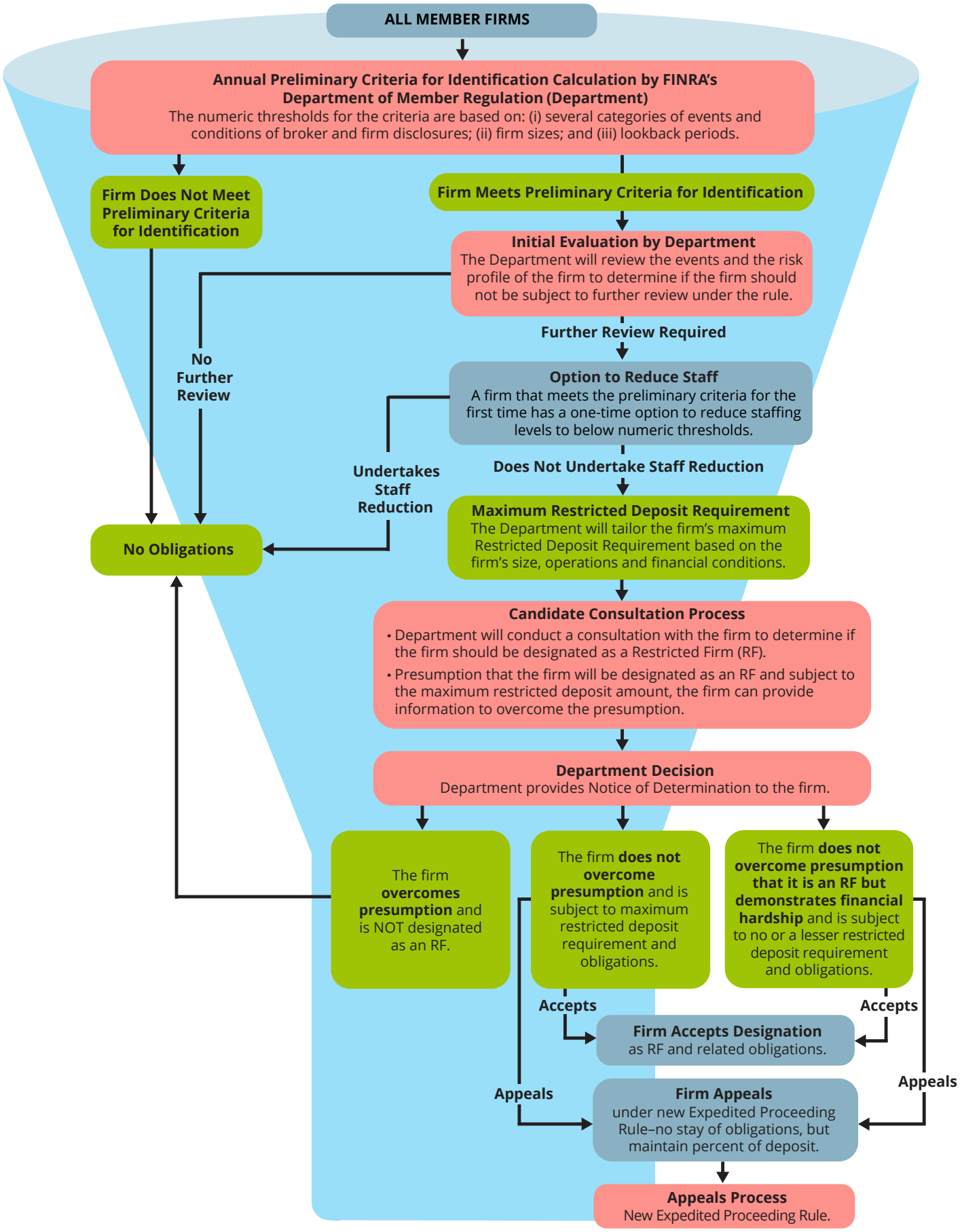
(1) through (9) No Change.

(b) No Change.

* * * * *

Attachment B

Rule 4111 (Restricted Firm Obligations)



Considerations and Practices for Supervising Independent Contractors

Tuesday, May 17, 2022
9:45 a.m. – 10:45 a.m.

This panel of FINRA staff and industry members addresses common challenges in supervising independent contractors. The session offers examples and suggestions for firms to use in their everyday supervision and compliance efforts. The panel also discusses existing rules and related guidance and shares effective industry practices.

Moderator:

Todd Coppi
Director, Retail Firm Examinations
FINRA Member Supervision

Panelists:

Robert Molinari
Chief Regulatory Affairs Officer
Commonwealth Financial Network

Meaghan Reim-Strange
Senior Principal Examiner, Retail Firm Examinations
FINRA Member Supervision

Douglas Wilburn
General Counsel and Chief Compliance Officer
Valmark Securities, Inc.

Considerations and Practices for Supervising Independent Contractors Panelists Bios:

Moderator:

Todd J. Coppi has been employed with FINRA for more than 22 years and is currently an Examination Director in the Boston Office. Prior to joining FINRA, Mr. Coppi was employed with Dreyfus Service Corporation (acting Branch Manager) and Morgan Stanley Dean Witter as a Financial Consultant. As Examination Director, Mr. Coppi is responsible for the execution of Member Supervision's examination program relative to a subset of firm types and business models, primarily those firm conducting retail sales, and manages a number of Member Supervision staff located throughout the Northeast. Mr. Coppi has a bachelor's degree in business administration from Mt. Ida College in Newton, MA and is also a graduate of the FINRA Institute at Wharton Certified Regulatory and Compliance Professional™ (CRCP™) program.

Panelists:

Robert Molinari has been with Commonwealth Financial Network since 2004. As the Chief Regulatory Affairs Officer, Mr. Molinari leads and manages the Regulatory Response Unit and oversees management of the Supervisory Controls Unit, which performs 3120 and 206(4)-7 testing at the firm. He received his BS in criminal justice from Northeastern University and his MBA from Babson College. In addition, Mr. Molinari holds the Certified Regulatory and Compliance Professional (CRCP)® designation, as well as a number of FINRA registrations.

Meaghan Reim-Strange is Senior Principal Examiner, Member Supervision for FINRA. Ms. Reim-Strange's responsibilities include: (i) serving primarily as lead examiner and point of contact for examinations of FINRA member Firms; Investigate FINRA member Firm's processes and procedures in areas such as AML Compliance, Supervisory Controls; Private Securities Transactions; Outside Business Activities; Consolidated Statements; Excessive Trading and Churning; (ii) analyzing examination findings and member Firm regulatory history to determine appropriate disposition; and (iii) provides on the job training for newer examiners. Ms. Reim-Strange has been with FINRA since 2010. She entered the securities industry in 2002 as a broker-trainee before moving to an Equity Capital Markets Compliance Associate position for a broker dealer within the Philadelphia area. Ms. Reim-Strange has a Bachelor of Arts degree in Political Science from Villanova and a Juris Doctor from Widener University School of Law. She has been a member of the Pennsylvania bar since 2009 and she is also a Certified Fraud Examiner (CFE).

Doug Wilburn is General Counsel and Chief Compliance Officer of Akron, Ohio-based Valmark Financial Group and its broker-dealer, Valmark Securities, and investment adviser, Valmark Advisers. Mr. Wilburn received his undergraduate degree in Political Science from the University of Missouri and, immediately upon graduating from St. Louis University School of Law, began his career in financial services at AG. Edwards & Sons. Mr. Wilburn later went on to practice law in both the public and private sectors, first as a public defender and then as an associate in the Litigation Department of St. Louis, Missouri-based Bryan Cave. Mr. Wilburn was subsequently appointed Missouri Securities Commissioner where he led his state's investor education efforts while also enforcing its securities laws. Mr. Wilburn then went on to serve as Managing Director and Deputy Chief Compliance Officer at Wachovia Securities in Richmond, Virginia and then as the Chief Compliance officer of Washington Mutual's retail broker-dealer and investment adviser in Irvine, California. Upon JP Morgan Chase's acquisition of Washington Mutual, Mr. Wilburn was named Managing Director and Chief Compliance officer of JP Morgan Chase's retail broker-dealer and investment adviser, Chase Investment Services. Mr. Wilburn holds Series 4, 7, 14, 24 and 66 registrations.

Considerations and Practices for Supervising Independent Contractors

Panelists

- **Moderator**
  - Todd Coppi, Director, Retail Firm Examinations, FINRA Member Supervision
- **Panelists**
  - Robert Molinari, Chief Regulatory Affairs Officer, Commonwealth Financial Network
  - Meaghan Reim-Strange, Senior Principal Examiner, Retail Firm Examinations, FINRA Member Supervision
  - Douglas Wilburn, General Counsel and Chief Compliance Officer, Valmark Securities, Inc.

To Access Polling

- **Please get your devices out:**
  - Type the polling address, **https://finra.cnf.io/sessions/nqxm** into the browser or scan the QR code with your camera.

  - Select your polling answers.

Polling Question 1

1. **What size firm are you from?**
   a. 1-100 RRs
   b. 101-500 RRs
   c. 500-5000 RRs
   d. Over 5,000 RRs

Polling address: **https://finra.cnf.io/sessions/nqxm**

Polling Question 2

2. What supervisory structure does your firm employ?

a. Centralized (A separate unit within the main/home office dedicated to overseeing specific functions such as trade review; account review; correspondence; and/or advertising. All supervisory reviews are submitted to and reviewed by this unit/group.)
b. Hub and Spoke (Centrally located OSJs that supervise the branch office activity of several branches that report into the OSJ.)
c. Decentralized (OSJs and/or branches are responsible for the review and approval of all functions at the branch office location such as trade review; account review; correspondence and/or advertising.)
d. Hybrid: Supervision duties are split between A, B, and/or C.

Polling address: **https://finra.cnf.io/sessions/nqxm**

Polling Question 3

3. **To what extent does your firm use automated surveillance (technology) to supervise transactions?**
   a. Most surveillance is automated
   b. Some surveillance is automated
   c. Manual surveillance

Polling address: **https://finra.cnf.io/sessions/nqxm**

Polling Question 4

4. **What best describes your firm's approach relative to OBA/PST?**
   a. We do not permit OBA/PST
   b. We permit limited OBA/PST (Fixed Insurance, Professional Services, etc.)
   c. We permit most OBA/PST

Polling address: **https://finra.cnf.io/sessions/nqxm**

Polling Question 5

5. **To what degree do you control the security protocols on devices used by your firm's APs?**
   a. All RRs use devices provided by the firm with built-in security protocols
   b. RRs use their own devices but with significant firm-imposed security protocols
   c. RRs use their own devices but with some firm-imposed security protocols
   d. RRs use their own devices with no firm-imposed security protocols

Polling address: **https://finra.cnf.io/sessions/nqxm**

Considerations and Practices for Supervising Independent Contractors
Tuesday, May 17, 2022
9:45 a.m. – 10:45 a.m.

Resources:

- FINRA *Regulatory Notice 20-16, FINRA Shares Practices Implemented by Firms to Transition to, and Supervise in, a Remote Work Environment During the COVID-19 Pandemic* (May 2020)

  www.finra.org/rules-guidance/notices/20-16

- FINRA *Regulatory Notice 18-08*, *FINRA Requests Comment on Proposed New Rule Governing Outside Business Activities and Private Securities Transactions* (February 2018)

  www.finra.org/sites/default/files/notice_doc_file_ref/Regulatory-Notice-18-08.pdf

- FINRA Rule 3270, *Outside Business Activities of Registered Persons*

  www.finra.org/rules-guidance/rulebooks/finra-rules/3270

- FINRA Rule 3280, *Private Securities Transactions of an Associated Person*

  www.finra.org/rules-guidance/rulebooks/finra-rules/3280

- Remote Branch Office Inspections

  www.finra.org/about/finra-360/progress-report/remote-branch-office-inspections

Trends and Developments in Private Placements
Tuesday, May 17, 2022
11:00 a.m. – 12:00 p.m.

This session focuses on industry and regulatory developments related to private placements. During the session, panelists discuss common concerns and recent regulatory findings. Speakers provide practical information and compliance tips for firms offering these products and discuss *Regulatory Notice 21-10*.

Moderator:
Minh Le
Director, Private Placements
FINRA Corporate Financing

Panelists:
Kimberly Flanders
Associate Director
FINRA Advertising Regulation

Tyler Gray
President
MicroVentures Marketplace Inc.

Scott Maestri
Director, Retail Firm Examinations
FINRA Member Supervision

Trends and Developments in Private Placements Panelists Bios:

Moderator:

Minh Q. Le is Director of FINRA's Corporate Financing Department. He has more than 20 years of experience in the regulation of public and private offerings. Currently, Mr. Le manages the department's Private Placement Review program which conducts regulatory oversight of broker-dealer participation in retail private offerings. In addition to overseeing the review and investigation program, Mr. Le's duties include developing policy and providing guidance on corporate financing and other capital-raising related issues. Mr. Le also routinely provides subject matter expertise to FINRA's Examination and Enforcement staffs. Building on this experience, Mr. Le serves as a member on FINRA's Regulatory Specialist committees for Public Offerings, Private Placements, and Non-traded Direct Participation Programs (DPP) and Real Estate Investment Trusts (REIT), and was a member of FINRA's Risk Assessment Committee. For the past 19 years, he has been a member of FINRA's Sales Rep and DPP/REIT Qualifications Committees. Prior to his involvement in developing FINRA's private placement rules and the filing program, Mr. Le was a manager in the department's Public Offerings Review program, which is responsible for regulating underwriting terms and arrangements in public offerings. Mr. Le graduated from the University of Maryland, attended the Wharton Institute of Executive Education, and is a Certified Regulatory and Compliance Professional (CRCP)®.

Panelists:

Kimberly Flanders is Associate Director in FINRA's Advertising Regulation Department. Her chief responsibility is managing staff members dedicated to the review of matters involving complex products and novel regulatory concerns. Ms. Flanders joined FINRA (f/k/a NASD) in March 1995 as an examiner in the Enforcement Department. She joined the Advertising Regulation Department in March 1996. In January 2001, Ms. Flanders joined Bisys Services as a senior advertising regulation consultant. Ms. Flanders returned to the Advertising Regulation Department in September 2001. Prior to joining FINRA, she was an investigator with the Resolution Trust Corporation. Ms. Flanders received a B.A. from the University of Georgia.

Tyler Gray is President of MicroVenture Marketplace Inc., an alternative investment platform democratizing the private markets. He is responsible for the Firm's strategic direction, vision, growth, and performance. In his previous role with the firm, he was the Chief Operating Officer overseeing back-office operations, platform development, marketing, and finance. He has been with the firm since 2013 and has also previously served as the firm's Chief Compliance Officer. He holds a BA in Economics from Michigan State University and an MBA with a concentration in Accounting from St. Edward's University. Additionally, he holds the Series 7, 9, 10, 24, 27, 63 and 99 licenses.

Scott H. Maestri is Examination Director located in FINRA's Dallas Office. He began his career with NASD in 1999 as an examiner in the New Orleans District Office. Mr. Maestri was promoted to management in September of 2003 and became responsible for a team of examiners who monitored member firms through cycle and cause investigations, as well as, the Membership Application Process and Financial Surveillance. Mr. Maestri was promoted to the Associate District Director position in May of 2010 where his primary responsibility was the review and approval of the District Office's major program areas. Beginning in 2020, Mr. Maestri's role changed to focus on leading a team of four managers and 20 examiners located throughout the country who are responsible for conducting examinations of firms with a retail business model. Prior to NASD, Mr. Maestri worked in a variety of sales, operational, and compliance roles with both Morgan Stanley and Legg Mason in the Jackson, Mississippi branch office locations. During the course of his career, Mr. Maestri has been selected for Advanced Management training, and successfully obtained the Certified Regulatory and

Compliance Professional™ (CRCP™) designation both issued through The Wharton School at the University of Pennsylvania. Mr. Maestri received his B.B.A. in Finance from The Else School of Management at Millsaps College.

Trends and Developments in Private Placements

Panelists

- **Moderator**
  - Minh Le, Director, Private Placements, FINRA Corporate Financing
- **Panelists**
  - Kimberly Flanders, Associate Director, FINRA Advertising Regulation
  - Tyler Gray, President, MicroVentures Marketplace Inc.
  - Scott Maestri, Director, Retail Firm Examinations, FINRA Member Supervision

Trends and Developments in Private Placements
Tuesday, May 17, 2022
11:00 a.m. – 12:00 p.m.

Resources:

- FINRA Frequently Asked Questions Related to Filing Requirements of Rules 5122 and 5123

  www.finra.org/rules-guidance/guidance/faqs/finra-rules-5122-5123

- FINRA Frequently Asked Questions on Rule 2210

  www.finra.org/rules-guidance/guidance/faqs/advertising-regulation

Regulatory Notice 20-21

Communications With the Public

FINRA Provides Guidance on Retail Communications Concerning Private Placement Offerings

July 1, 2020

Notice Type
- Guidance

Suggested Routing
- Advertising
- Compliance
- Corporate Financing
- Legal
- Operations
- Registered Representatives
- Senior Management

Key Topics
- Communications with the Public
- Private Placements
- Retail Communications

Referenced Rules
- FINRA Rule 2210
- Regulation D
- Regulatory Notice 10-22
- Regulatory Notice 13-18
- Regulatory Notice 19-31

Summary

This *Notice* provides guidance to help member firms comply with FINRA Rule 2210, Communications with the Public, when creating, reviewing, approving, distributing, or using retail communications concerning private placement offerings.

Questions concerning this *Notice* should be directed to:

- Amy C. Sochard, Vice President, Advertising Regulation, at (240) 386-4508; or
- Ira D. Gluck, Director, Advertising Regulation, at (240) 386-4614.

Background and Discussion

Private Placement Offerings

Private placements are unregistered, non-public securities offerings that rely on an available exemption from registration with the Securities and Exchange Commission (SEC) under either Sections 3 or 4 of the Securities Act of 1933 (Securities Act).[1] Most private offerings, however, are sold pursuant to one of three "safe harbors" under Rules 504, 506(b), and 506(c) of Securities Act Regulation D (Reg D).[2]

Reg D requires companies and funds to file a Form D through the SEC's EDGAR system when selling unregistered securities based on a claimed Reg D exemption. The most recent Reg D data published by the SEC's Division of Economic and Risk Analysis indicates that issuers make approximately 20,000 new offering Reg D filings with the SEC each year.[3] Of this total, approximately 4,000 new offerings identify an "intermediary," such as a broker or finder, as participating in an offering.

Private placements sold by FINRA member firms to individuals generally must be filed with FINRA. In this regard, FINRA Rules 5122 and 5123 require a member firm to file offering documents regarding specified private placements in which the member firm participates.[4] FINRA receives

approximately 2,000 new offering filings from its member firms each year,[5] and uses analytics and trained analysts to conduct a risk-based review of each filing. The number of annual filings with FINRA indicates that approximately half of the Reg D filings identifying intermediaries are for offerings by entities that are not subject to FINRA rules or offerings by member firms that are not required to file under Rules 5122 or 5123.

The offerings that are sold directly by issuers or through the efforts of intermediaries that are not FINRA member firms are not subject to the regulatory requirements applicable under FINRA rules and are not subject to FINRA's examination and review programs. Although FINRA does not have jurisdiction over Reg D private placements that are sold directly to investors or through non-member firm intermediaries, it is committed to promoting investor protection through meaningful regulation and oversight of member firms participating in these offerings.

The remainder of this *Notice* addresses the subset of private placements conducted by member firms.

Private Placement Retail Communications

Many private placement offerings to retail investors include marketing or sales communications that meet the definition of retail communication in Rule 2210(a)(5).[6] For example, FINRA has observed that more than 40 percent of the offerings filed pursuant to FINRA Rule 5123 include retail communications. In addition, the adoption of Rule 506(c) under Reg D eliminated the prohibition against general solicitation and advertising for private placement offerings where all purchasers of the securities are verified accredited investors. Consequently, member firms have become increasingly involved in the distribution of private placement securities through online platforms and other widely disseminated communications such as digital advertisements.[7]

FINRA Rule 2210(d)(1) requires that all member firm communications be fair, balanced and not misleading. Communications that promote the potential rewards of an investment also must disclose the associated risks in a balanced manner.[8] In addition, communications must be accurate and provide a sound basis to evaluate the facts with respect to the products or services discussed. Rule 2210(d)(1) also prohibits false, misleading or promissory statements or claims, and prohibits the publication, circulation or distribution of a communication that a member firm knows or has reason to know contains any untrue statement of a material fact or is otherwise false or misleading. With few exceptions, Rule 2210(b)(1) requires that an appropriately registered principal approve each retail communication before the earlier of its use or filing with FINRA's Advertising Regulation Department.[9]

Recent FINRA reviews of retail communications concerning private placements have revealed deficiencies. For instance, most if not all investments in private placements are illiquid, and many such investments are speculative in nature. Some retail communications do not balance claims of these investments' benefits by disclosing these risks. Others have contained false, misleading, or promissory statements or claims such as assertions about the likelihood of a future public offering of the issuer, claims about the future success of the issuer's new or untried business model, inaccurate or misleading assertions concerning the regulation or relative risk of the offering, or predictions or projections of investment performance prohibited by FINRA Rule 2210(d)(1)(F).

FINRA is providing the following guidance to assist member firms in their creation, review, approval, distribution or use of retail communications concerning private placement securities.

Third-Party Prepared Materials

Rule 2210(a)(5) defines "retail communication" as "any written (including electronic) communication that is ***distributed or made available*** to more than 25 retail investors within any 30 calendar-day period."[10] FINRA disciplinary actions demonstrate that member firms can be liable for violations of Rule 2210 when distributing or using noncompliant retail communications prepared by a third party.[11]

Regulatory Notice 10-22 states that "[a member firm] that assists in the preparation of a private placement memorandum or other offering document should expect that it will be considered a communication with the public by that [member firm] for purposes of ... Rule 2210, FINRA's advertising rule. If a private placement memorandum or other offering document presents information that is not fair and balanced or that is misleading, then the [member firm] that assisted in its preparation may be deemed to have violated ... Rule 2210." *Notice 10-22* also provides that "sales literature concerning a private placement that a [member firm] distributes will generally be deemed to constitute a communication by that [member firm] with the public, whether or not the [member firm] assisted in its preparation."

In addition, FINRA has observed that some issuer-prepared private placement memoranda (PPMs) are bound or presented as one electronic file with retail communications, such as cover pages or exhibits. Such retail communications are distinguishable by their marketing or promotional content from the factual descriptions and financial information about the issuer generally disclosed in the PPMs. Regardless of whether a member firm distributes a retail communication that is attached to a PPM or as a standalone document, it constitutes a communication of the member firm subject to Rule 2210.

Balanced Presentation of Risks and Investment Benefits

Rule 2210 requires communications that discuss the benefits of an investment also to include a discussion of its risks.[12] As indicated above, retail communications that discuss the potential benefits of investing in private placements should balance this discussion with disclosure of their risks, such as the potential for private placement investments to lose value, their lack of liquidity and their speculative nature. Providing risk disclosure in a separate document, such as a PPM, or in a different section of a website does not substitute for disclosure contained in or integrated with retail communications governed by Rule 2210.

Retail communications often highlight the business of the issuer and discuss the value proposition of a potential investment. In such cases, the key risks associated with an investment in the issuer are necessary in order to balance the positive portrayal of the investment. For example, when the issuer is a startup company, the risks may include a limited track record; more experienced or larger competitors; overreliance on financing; reliance on a single supplier, customer or employee; or lack of management experience.

Reasonable Forecasts of Issuer Operating Metrics

Rule 2210(d)(1)(F) generally prohibits the use of any prediction or projection of performance, as well as any exaggerated or unwarranted claim, opinion or forecast.[13] Accordingly, retail communications concerning private placements may not project or predict ***returns to investors*** such as yields, income, dividends, capital appreciation percentages or any other future investment performance.

However, FINRA would not consider reasonable forecasts of ***issuer operating metrics*** (*e.g.*, forecasted sales, revenues or customer acquisition numbers) that may convey important information regarding the issuer's plans and financial position to be inconsistent with the rule. Presentations of reasonable forecasts of issuer operating metrics should provide a sound basis for evaluating the facts as required by Rule 2210(d)(1)(A). For example, such presentations should include clear explanations of the key assumptions underlying the forecasted issuer operating metrics and the key risks that may impede the issuer's achievement of the forecasted metrics.

When creating, reviewing, approving, distributing or using forecasts of issuer operating metrics in retail communications, member firms should consider:

I. the time period forecasted (generally a time period in excess of five years would be unreasonable);

II. whether growth rate assumptions are commensurate with the nature and scale of the business;

III. whether forecasted gross margins[14] are commensurate with industry averages; and

IV. whether sales and customer acquisition forecasts are reasonable in relation to the overall market for the issuer's products or services.

While sources of contractual revenue such as royalty or master lease agreements may inform or provide a basis for reasonable forecasts of issuer operating metrics, it would be inconsistent with Rule 2210(d)(1)(B) to characterize specific revenue or cash flow as guaranteed or certain. Moreover, Rule 2210(d)(1)(F) precludes member firms from using the data from forecasts of issuer operating metrics to project or depict specific investment returns to an investor.

Distribution Rates

Regulatory Notice 13-18 provided guidance to member firms regarding communications with the public for registered and unregistered real estate investment programs. Given that some non-real estate private placement investments employ similar structures, the principles relating to distribution rates contained in that *Notice* are applicable to retail communications regarding private placement investments designed to provide distributions to investors and are reiterated below.

Some issuers fund a portion of their distributions through return of principal or loan proceeds. For example, a portion of a newer program's distributions might include a return of principal until its assets are generating significant cash flows from operations. Consistent with Rule 2210(d)(1)(B)'s prohibition of false, exaggerated, unwarranted, promissory or misleading claim, member firms must not misrepresent the amount or composition of such distributions. Nor may member firms state or imply that a distribution rate is a "yield" or "current yield" or that investment in the program is comparable to a fixed income investment such as a bond or note. Presentations of distribution rates consistent with Rule 2210 would disclose:

- that distribution payments are not guaranteed and may be modified at the program's discretion;
- if the distribution rate consists of return of principal (including offering proceeds) or borrowings, a breakdown of the components of the distribution rate showing what portion of the quoted percentage represents cash flows from the program's investments or operations, what portion represents return of principal, and what portion represents borrowings;
- the time period during which the distributions have been funded from return of principal (including offering proceeds), borrowings or any sources other than cash flows from investment or operations;
- if the distributions include a return of principal, that by returning principal to investors, the program will have less money to invest, which may lower its overall return; and
- if the distributions include borrowed funds, that since borrowed funds were used to pay distributions, the distribution rate may not be sustainable.[15]

FINRA believes that it is inconsistent with Rule 2210(d)(1) for retail communications to include an annualized distribution rate until the program has paid distributions that are, on an annualized basis, at a minimum equal to that rate for at least two consecutive full quarterly periods.[16]

Internal Rate of Return

Internal Rate of Return (IRR) is a measure of performance commonly used in connection with marketing private placements of real estate, private equity and venture capital. IRR shows a return earned by investors over a particular period, calculated on the basis of cash flows to and from investors (*i.e.,* the percentage rate earned on each dollar invested for each period the dollar was invested). IRR is calculated as the discount rate that makes the net present value of all cash flows from an investment equal to zero.[17]

A drawback of IRR calculations is their inherent assumption that investors will be able to reinvest any distributions from the investment at the IRR rate. In practice, it is unlikely that this would occur. Another drawback is that in order to calculate IRR for a portfolio that includes holdings that have not yet been sold (or otherwise liquidated or matured), a valuation of those remaining assets must be estimated. Depending on the nature of the asset, these estimated values may be based on subjective factors and assumptions.

The use of IRR in retail communications concerning privately placed new investment programs that have no operations or that operate as a blind pool would be inconsistent with the prohibition on unwarranted forecasts or projections in Rule 2210(d)(1)(F).

Nevertheless, FINRA interprets Rule 2210 to permit retail communications to include IRR for completed investment programs (*e.g.,* the holding matured or all holdings in the pool have been sold). In addition, FINRA does not view as inconsistent with the rule retail communications that provide an IRR for a specific investment in a portfolio if the IRR represents the actual performance of that holding.

Investment programs such as private equity funds and REITs may have a combination of realized investments and unrealized holdings in their portfolios. Where the program has ongoing operations, FINRA interprets Rule 2210 to permit the inclusion of IRR if it is calculated in a manner consistent with the Global Investment Performance Standards (GIPS) adopted by the CFA Institute and includes additional GIPS-required metrics such as paid-in capital, committed capital and distributions paid to investors.[18]

Endnotes

1. *See* 15 U.S.C. 77c and 77d.
2. *See* 17 CFR 230.504, 230.506(b) and 230.506(c).
3. *Capital Raising in the U.S.: An Analysis of the Market for Unregistered Securities Offerings, 2009-2017:* https://www.sec.gov/dera/staff-papers/white-papers/dera_white_paper_regulation_d_082018.
4. Rules 5122 and 5123 provide exemptions from the filing requirement when certain types of securities are sold or securities are sold to certain types of investors. For example, member firms are not required to file offerings made pursuant to Securities Act Rule 144A or Regulation S, or offerings sold solely to institutional accounts as defined in FINRA Rule 4512(c). *See* Rules 5122(c) and 5123(b). As a result of these exemptions, both rules apply predominately to retail private placements.
5. The total for "new offering filings" excludes duplicate filings for the same offering by different member firms.
6. "Retail communication" means any written (including electronic) communication that is distributed or made available to more than 25 retail investors within any 30 calendar-day period.
7. *See* FINRA's 2019 Annual Risk Monitoring and Examinations Priorities Letter (January 2019). The letter discusses factors FINRA may consider in reviewing online distribution platforms.
8. *See Regulatory Notice 19-31* (September 19, 2019), Question 3 ("FINRA rules require that communications be fair and balanced, but don't require them to be exhaustive lists of all possible risks and warnings associated with a product or service. Information about risks, costs or drawbacks is more effective when it is related to the benefits that the communication promotes.").
9. For example, pursuant to Rule 2210(b)(1)(C), if a member firm has already filed a retail communication with FINRA's Advertising Regulation Department and received a letter indicating that such communication appears to be consistent with applicable standards, another member firm may use that communication without having a principal approve it, provided the communication is not materially altered or used in a manner that is inconsistent with the department's letter.
10. Emphasis added. Rule 2210's definitions of correspondence and institutional communications also refer to communications that are "distributed or made available" to particular investors. *See* FINRA Rules 2210(a)(2) and (a)(3).
11. *See e.g., Phillipe N. Keyes*, 89 S.E.C. 792, 800 (2006), *Sheen Financial Resources, Inc.,* Exchange Act Release No. 35477, 52 SEC 185, SEC LEXIS 613 (1995), Fidelity Brokerage Services LLC, Letter of Acceptance, Waiver and Consent No. 2008013056101 (2011) or HSBC Securities (USA) Inc., Letter of Acceptance Waiver and Consent No 008013863801 (2010).
12. *See* FINRA Rule 2210(d)(1)(D).
13. Rule 2210(d)(1)(F) contains three exceptions from this prohibition, subject to specified conditions: (1) hypothetical illustrations of mathematical principles; (2) investment analysis tools and reports generated by such tools; and (3) a price target contained in a research report.
14. Gross margin represents the percent of total sales revenue that the company retains after incurring the direct costs associated with producing the goods and services sold by a company. *See Jay Michael Fertman*, 51 SEC 943,950 (1994) and *Excel Fin., Inc.,* 53 SEC 303, 311-12 (1997).

15. *See* *Regulatory Notice 13-18* (May 2013).

16. *Id.* "In order to be fair and balanced, firm communications concerning a real estate program may not include an annualized distribution rate until the program has paid distributions that are, on an annualized basis, at a minimum equal to that rate for at least two consecutive full quarterly periods."

17. IRR is also known as money-weighted returns. This can be contrasted to a time-weighted return, which is the compounded growth rate of $1 over the time period. Average annual total returns used by mutual funds pursuant to SEC Rule 482 are an example of time-weighted returns. Time-weighted returns ignore the size and timing of investment cash flows and therefore provide a measure of manager or strategy performance, while IRR measures how a specific portfolio performed in absolute terms.

18. The CFA Institute is a global association of investment professionals. *See generally* CFA Institute Global Investment Performance Standards.

Regulatory Notice 21-10

Private Placement Filer Form

FINRA Updates Private Placement Filer Form Pursuant to FINRA Rules 5122 and 5123

Effective Date: May 22, 2021

March 11, 2021

Notice Type
- Guidance

Suggested Routing
- Compliance
- Corporate Finance
- Legal
- Operations
- Private Placement
- Registered Representatives
- Senior Management
- Underwriting

Key Topics
- Private Placement
- Underwriting

Referenced Rules & Notices
- FINRA Rule 3280
- FINRA Rule 5122
- FINRA Rule 5123
- Regulatory Notice 10-22

Summary

FINRA has updated the form that members must use to file offering documents and information pursuant to FINRA Rules 5122 (Private Placements of Securities Issued by Members) and 5123 (Private Placements of Securities) (Filer Form). The updated Filer Form will be accessible in the FINRA Gateway beginning May 22, 2021, and includes new and updated questions that will facilitate review of the filed material.[1] Beginning on May 22, 2021, members will be required to complete the updated Filer Form for all new filings, as well as for new amendments to filings.

See Attachment A for a copy of the updated Filer Form. In addition, this *Notice* informs members about the information that may be requested during a FINRA examination concerning the member's private placement business. *See* Attachment B for a copy of the "Unregistered Offering List" template.

Questions regarding this *Notice* may be directed to:

- Minh Le, Director, Corporate Financing, at (240) 386-4638 or *Minh.Le@finra.org*;
- Janet Boysen, Manager, Corporate Financing, at (240) 386-5101 or *Janet.Boysen@finra.org*; or
- Kathryn Moore, Associate General Counsel, Office of General Counsel, at (202) 728-8200 or *Kathryn.Moore@finra.org*.

Background and Discussion

FINRA Rule 5122 establishes disclosure and filing requirements for members that sell a private placement of an unregistered security issued by a broker-dealer or a control entity. Its companion rule, FINRA Rule 5123, requires members that sell a private placement to file a copy of any offering documents with FINRA within 15 calendar days of the first sale, subject to various exemptions.[2] FINRA requires members to submit the Filer Form that contains information about the member selling the private placement

securities, the issuer and the offering terms as well as any offering documents, if applicable, electronically through the FINRA Gateway.[3] If more than one firm is selling, a firm can make the required filing on behalf of others.

The Filer Form has three main components: the "Participating Member Information" section; the "Issuer Information" section; and the "Offering Information" section.

On May 22, 2021, FINRA will begin using an updated Filer Form that adds new questions, and clarifies certain existing questions and requests for information in the Offering Information section. The updates are designed to enhance oversight in particular areas of risk in the private placement market. Collecting targeted information in these areas will enhance investor protection and efficiency. For example, the updated Filer Form addresses the most relevant information at the outset, reducing the possibility that members will need to respond to additional FINRA information requests. FINRA describes these changes below. Attachment A is a copy of the revised Filer Form.

Contingency Offerings

FINRA is adding the following questions concerning contingency offerings:

- the date by which the contingency must be met;
- whether there have been any changes to the original terms of the contingency during the course of the offering (*e.g.,* extension of the date by which the contingency must be met); and
- whether the subscription process involves the member receiving or transmitting investor funds in the offering. If so, there will be a follow-up question to identify what entity is acting as the escrow agent or trustee for investor funds, and to provide the name of the escrow agent if applicable.

Disciplinary History of the Issuer, its Principals and Affiliates

FINRA is adding questions to obtain clarification on the disciplinary history of the issuer, the issuer's principals and affiliates. FINRA reminds members of their obligation to conduct a reasonable investigation of the issuer and securities they recommend.[4]

FINRA is amending the existing question to include actions or proceedings involving any federal agency, not just the SEC. The revised question is as follows (changes in bold):

> Has the issuer, any officer, director or executive management of the issuer, sponsor, general partner, manager, advisor or any of the issuer's affiliates been the subject of FINRA, SEC **or other federal agency**, or state disciplinary actions or proceedings or criminal complaints within the last 10 years?

If the member answers yes, this section will request identifying information about the person or entity that is the subject of the action, proceeding or complaint. If such person or entity has registration records in CRD, the member may enter the CRD information for identification purposes and there are no further questions. Otherwise, the section will request the name of the individual or entity with the disciplinary history; additional information concerning the type of proceeding (*e.g.,* FINRA, federal agency, state, criminal); the approximate date of the proceeding; and the current status.

Intended Use of Proceeds

FINRA is amending the question about the intended use of offering proceeds as follows (changes in bold):

> **Does the issuer intend** to use offering proceeds to make or repay loans to, purchase assets from, or **otherwise direct investor proceeds** to any officer, director, or executive management of the issuer, sponsor, general partner, manager, advisor, or any of the Issuer's affiliates?

If the member responds yes to this question, this section will request additional information concerning the type of payment and approximate dollar amount of offering proceeds that is intended for that purpose. The responsibility of members to conduct a reasonable investigation of the offering includes review of the intended use of proceeds.[5]

Private Securities Transactions

The Offering Information section also asks the member to identify whether the filing is for an offering that its associated person is selling in a private securities transaction subject to FINRA Rule 3280.

Additional Changes

FINRA is also making changes to three existing questions in order to clarify the information requested, make relevant updates, and improve data collection.

First, FINRA asks whether the member has commenced sales (applicable to FINRA Rule 5123 filings) or offers or provided offering documents to investors (FINRA Rule 5122 filings). If yes, FINRA will request the date of first sale (or offer or provided documents).

Second, the Offering Information section removes Rule 505 from the list of exemptions from registration. Rule 505 was repealed in 2016 and is no longer an available exemption.

Finally, the Filer Form amends the process by which the member uploads offering documents that it used in connection with the sale of the offering. For each document that the member uploads, the Filer Form requests that the member identify the type of document using a check-box. The member has the option to select more than one type of document.

Member Supervision Examinations

In keeping with the changes to the Filer Form discussed above, FINRA believes that additional transparency on examinations of members that conduct private placement business may promote efficiency. During the course of an examination of a member that engages in a private placement business, FINRA staff may request information related to that activity. These requests generally seek information not already provided by members in their FINRA Rule 5122 and 5123 filings, and in some cases may include offerings exempted from filing under FINRA Rules 5122 or 5123.

Members that conduct a private placement business can expect FINRA staff to request a list of private placements they are selling or have sold and certain data pertaining to each. The staff uses this information to assess and evaluate the risks associated with the member's private placement activities. To assist members in preparing for these requests, please see Attachment B, "Unregistered Offering List Request" template, that lists the types of information that FINRA will request from members as part of an examination.

Endnotes

1. *See* Securities Exchange Act Release No. 91047 (February 3, 2021); 86 FR 8819 (February 9, 2021) (Notice of Filing and Immediate Effectiveness of File No. SR-FINRA-2021-002).
2. FINRA Rule 5123(a) requires broker-dealers to "provide FINRA with the required documents or notification and related information, if known, by filing an electronic form in a manner prescribed by FINRA."
3. If a member sells a private placement without using an offering document, the member must state that fact.
4. *See* Regulatory Notice 10-22 (April 2010).
5. *Id.*

Regulatory Notice 21-26

Private Placement Retail Communications

FINRA Amends Rules 5122 and 5123 Filing Requirements to Include Retail Communications That Promote or Recommend Private Placements

Implementation Date: October 1, 2021

July 15, 2021

Notice Type
- Rule Amendment

Suggested Routing
- Compliance
- Legal
- Operations
- Senior Management

Key Topics
- Advertising Regulation
- Communications with the Public
- Corporate Financing
- Private Placements
- Retail Communications

Referenced Rules and Notices
- FINRA Rule 2210
- FINRA Rule 4512
- FINRA Rule 5122
- FINRA Rule 5123
- FINRA Rule 5130
- Regulatory Notice 09-27
- Regulatory Notice 20-21
- Securities Act Rule 144A

Summary

FINRA has adopted changes to FINRA Rules 5122 (Private Placements of Securities Issued by Members) and 5123 (Private Placements of Securities) to require members to file retail communications that promote or recommend private placement offerings that are subject to those rules' filing requirements.[1] The new filing requirements become effective on October 1, 2021.

The amended text of the rules is set forth in Attachment A.

Questions concerning this *Notice* should be directed to:

- Paul Mathews, Vice President, Corporate Financing, at (240) 386-4639 or paul.mathews@finra.org;
- Amy Sochard, Vice President, Advertising Regulation, at (240) 386-4508 or amy.sochard@finra.org; or
- Joseph P. Savage, Vice President, Office of General Counsel, at (240) 386-4534 or joe.savage@finra.org.

Background and Discussion

FINRA Rules 5122 and 5123

Rule 5122 applies to private placements of unregistered securities issued by a member or a control entity[2] ("member private offerings"). The rule requires the member or control entity to provide prospective investors with a private placement memorandum (PPM), term sheet, or other offering document that discloses the intended use of the offering proceeds, the offering expenses and the amount of selling compensation that will be paid to the member and its associated persons.

The rule also requires a member to file the PPM, term sheet or other offering document with the FINRA Corporate Financing Department ("Corp Fin") at or prior to the first time the document is provided to any prospective investor.[3] Many member private offerings are exempt from the rule's requirements, including among others, offerings sold only to institutional accounts, as defined in FINRA Rule 4512(c),[4] qualified purchasers, as defined in the Investment Company Act of 1940,[5] and qualified institutional buyers,[6] as defined in Rule 144A under the Securities Act of 1933 ("Securities Act").[7]

Rule 5123 requires members to file with FINRA any PPM, term sheet or other offering document, including any material amended versions thereof, used in connection with a private placement of securities within 15 calendar days of the date of first sale. Rule 5123 exempts private placements that are filed under other FINRA Corporate Financing Rules, as well as most of the same categories of private placements that are exempt from filing under Rule 5122.[8] As a result of these exemptions, both rules apply predominately to private placements sold to retail investors.

Members that sell private placements may use a PPM or term sheet alone, or may use a variety of other offering documents in addition to, or instead of, a PPM or term sheet. Although, prior to these amendments, Rules 5122 and 5123 did not require retail communications governed by Rule 2210 (Communications with the Public) to be filed, many members filed these communications with their required documents.[9] Examples of these retail communications have included web pages, slide presentations, pitch decks, one-page "teasers," fact sheets, sales brochures, executive summaries and investor packets.[10]

FINRA has amended Rules 5122 and 5123 to require firms to file with Corp Fin retail communications that promote or recommend a private placement offering subject to those rules' filing requirements, in addition to the currently required PPMs, term sheets and other offering documents.[11] The amendments do not apply to any offerings that are currently exempt from filing, such as sales exclusively to institutional accounts.[12] The amendments will require a member to file such retail communications with Corp Fin no later than the date on which the member must file the private placement offering documents under Rules 5122 and 5123.[13]

FINRA expects that members will file most retail communications with Corp Fin at the same time and in the same manner that they file their PPMs, term sheets and other offering documents. The rules' requirements that members file material amendments to offering documents also will apply to material amendments to retail communications.

The amendments to FINRA Rules 5122 and 5123 become effective on October 1, 2021.

Endnotes

1. *See* Securities Exchange Act Release No. 92133 (June 9, 2021), 86 FR 31764 (June 15, 2021) (SR-FINRA-2020-038) (Order Approving a Proposed Rule Change, as Modified by Amendment No. 1, to FINRA Rules 5122 (Private Placements of Securities Issued by Members) and 5123 (Private Placements of Securities) That Would Require Members to File Retail Communications Concerning Private Placement Offerings That Are Subject to Those Rules' Filing Requirements).

2. A "control entity" means any entity that controls or is under common control with a member, or that is controlled by a member or its associated persons. *See* FINRA Rule 5122(a)(2). Control means beneficial interest, as defined in FINRA Rule 5130(i)(1), of more than 50 percent of the outstanding voting securities of a corporation, or the right to more than 50 percent of the distributable profits or losses of a partnership or other non-corporate legal entity. Control is determined immediately after the closing of an offering, and in the case of an offering with multiple intended closings, immediately following each closing. *See* FINRA Rule 5122(a)(3).

3. Rule 5122 also requires the filing of any amendments or exhibits to such documents within 10 days of being provided to any investor or prospective investor. *See* FINRA Rule 5122(b)(2).

4. Rule 4512(c) defines "institutional account" as the account of:

   (1) a bank, savings and loan association, insurance company or registered investment company;

   (2) an investment adviser registered either with the SEC under Section 203 of the Investment Advisers Act or with a state securities commission (or any agency or office performing like functions); or

   (3) any other person (whether a natural person, corporation, partnership, trust or otherwise) with total assets of at least $50 million.

5. *See* 15 U.S.C. 80a-2(a)(51).

6. *See* 17 CFR 230.144A(a)(1).

7. *See* Rule 5122(c) for a complete list of exempt member private offerings.

8. *See* FINRA Rule 5123(b) for a complete list of exempt private placements.

9. *Regulatory Notice 09-27* (May 2009), which announced SEC approval of Rule 5122, stated that the rule imposes no additional requirements regarding the filing of advertisements or sales materials. However, as noted, many firms have, in fact, filed retail communications that promote or recommend private placements under Rules 5122 and 5123.

10. In *Regulatory Notice 20-21* (July 1, 2020), FINRA provided guidance to help member firms comply with Rule 2210 when creating, reviewing, approving, distributing, or using retail communications concerning private placement offerings.

11. Members must file the offering documents and retail communications via FINRA's Private Placement Filing System in Firm Gateway.

12. *See supra* notes 7 and 8.

13. As discussed above, Rule 5122 requires a member subject to the rule to file the PPM, term sheet or other offering document with FINRA at or no later than the first time the document is provided to a prospective investor. Any amendments or exhibits to such offering documents also must be filed with FINRA within 10 days of being provided to any investor or prospective investor. *See* Rule 5122(b)(2). Rule 5123 requires a member subject to the rule to submit to FINRA, or have submitted on its behalf by a designated member, the PPM, term sheet or other offering document, including any materially amended versions thereof, used in connection with the sale of securities covered by the rule within 15 calendar days of the date of first sale, or notify FINRA that no such offering documents were used. *See* Rule 5123(a).

Attachment A

Below is the text of the proposed rule change. Proposed new language is underlined; proposed deletions are in brackets.

* * * * *

5100. SECURITIES OFFERINGS, UNDERWRITING AND COMPENSATION

5120. OFFERINGS OF MEMBERS' SECURITIES

* * * * *

5122. Private Placements of Securities Issued by Members

(a) No Change.

(b) Requirements

No member or associated person may offer or sell any security in a Member Private Offering unless the following conditions have been met:

(1) No Change.

(2) Filing Requirements

A member must file the private placement memorandum, term sheet, or [such] other offering document, and any retail communication (as defined under Rule 2210) that promotes or recommends the member private offering with the Corporate Financing Department at or prior to the first time the document or retail communication is provided to any prospective investor. Any amendment(s) or exhibit(s) to the private placement memorandum, term sheet, [or] other offering document or retail communication also must be filed with the Department within ten days of being provided to any investor or prospective investor.

(3) No Change.

(c) through (e) No Change.

• • • Supplementary Material: ----------

No Change.

5123. Private Placements of Securities

(a) Filing Requirements

Each member that sells a security in a non-public offering in reliance on an available exemption from registration under the Securities Act ("private placement") must: (i) submit to FINRA, or have submitted on its behalf by a designated member, a copy of any private placement memorandum, term sheet or other offering document, and any retail communication (as defined in Rule 2210) that promotes or recommends the private placement, including any materially amended versions thereof, used in connection with such sale within 15 calendar days of the date of first sale; or (ii) notify FINRA that no such offering documents or retail communications were used. Members must provide FINRA with the required documents, retail communications, or notification and related information, if known, by filing an electronic form in the manner prescribed by FINRA.

(b) through (d) No Change.

* * * * *

Enforcement Developments

Tuesday, May 17, 2022
11:00 a.m. – 12:00 p.m.

This session provides an overview of new developments and trends in enforcement, including enforcement priorities. Panelists highlight noteworthy decisions and settlements that illustrate FINRA priorities and provide guidance on regulatory and compliance practices.

Moderator:
Christopher Kelly
Senior Vice President and Deputy Head of Enforcement
FINRA Enforcement

Panelists:
Melissa Hodgman
Associate Director, Division of Enforcement
U.S. Securities and Exchange Commission (SEC)

Jessica Hopper
Executive Vice President and Head of Enforcement
FINRA Enforcement

Enforcement Developments Panelists Bios:

Moderator:

Christopher Kelly serves as Senior Vice President and Deputy Head of Enforcement. In that role, he oversees the work of the Main Enforcement staff who work from FINRA's headquarters in Maryland and New York, as well as the Sales Practice Enforcement staff in FINRA's 14 offices throughout the country. He joined FINRA in 2014 and served as Chief Counsel in FINRA's North Region until early 2018. Prior to joining FINRA, Mr. Kelly served as Deputy Chief of the Criminal Division at the U.S. Attorney's Office for the District of New Jersey. In that role, Mr. Kelly supervised more than 35 Assistant U.S. Attorneys in the Office's white collar units: Economic Crimes, National Security, Healthcare and Government Fraud, and Cybercrime. Prior to his promotion to the position of Deputy Chief, Mr. Kelly served as the Chief of the Economic Crimes Unit at the U.S. Attorney's Office, where he oversaw the Office's prosecution of complex economic crimes, including crimes involving insider trading, securities fraud, tax evasion, bank fraud, corporate fraud and embezzlement. Mr. Kelly also served as the lead prosecutor on numerous criminal prosecutions. Mr. Kelly graduated from Duke University and Harvard Law School. Prior to joining the U.S. Attorney's Office, he was an associate at the law firm Dechert LLP. Mr. Kelly also clerked for the Honorable Joseph E. Irenas, U.S. District Court Judge for the District of New Jersey.

Panelists:

Melissa R. Hodgman is Associate Director in the Division of Enforcement at the U.S. Securities and Exchange Commission. She joined the Commission in 2008, became Senior Counsel in 2009, joined the newly formed Market Abuse Unit in 2010, was promoted to Assistant Director in 2012, and to Associate Director in 2016. Ms. Hodgman served as the Acting Director of the Division of Enforcement at the U.S. Securities and Exchange Commission from January 2021 until July 2021. She was an Associate at Milbank, Tweed, Hadley & McCloy. She obtained a BSFS in 1990, a J.D., *magna cum laude,* in 1994, and an LL.M in Securities with Distinction in 2007 from Georgetown University.

Jessica Hopper is Executive Vice President and Head of Enforcement, responsible for FINRA's disciplinary actions across the country. Prior to assuming this role in January 2020, she was Senior Vice President and Deputy Head of Enforcement for four years, and Senior Vice President in charge of the Regional Enforcement program in the 14 FINRA District Offices from 2011 to 2016. Ms. Hopper joined FINRA in 2004 and was a Director in FINRA's Washington D.C. office until 2011. Prior to joining FINRA, from 2000 to 2004, she was part of Legg Mason Wood Walker, Inc.'s Legal & Compliance team, where her responsibilities focused on retail sales compliance. She began her career as a litigation attorney in private practice. Ms. Hopper holds a J.D. from the University of Toledo College of Law and earned a B.A. from Hillsdale College.

Enforcement Developments

Panelists

- **Moderator**
  - Christopher Kelly, Senior Vice President and Deputy Head of Enforcement, FINRA Enforcement
- **Panelists**
  - Melissa Hodgman, Associate Director, Division of Enforcement, U.S. Securities and Exchange Commission (SEC)
  - Jessica Hopper, Executive Vice President and Head of Enforcement, FINRA Enforcement

Regulatory Notice 19-23

FINRA Investigations

FINRA Supplements Prior Guidance on Credit for Extraordinary Cooperation

July 11, 2019

Notice Type
- Guidance

Suggested Routing
- Compliance
- Legal
- Operations
- Senior Management

Key Topic
- Extraordinary Cooperation

Referenced Rules & Notices
- FINRA Rule 4530
- FINRA Rule 8210
- FINRA Rule 8313
- Regulatory Notice 08-70
- Regulatory Notice 11-32
- Regulatory Notice 19-04
- Sanction Guidelines

Summary

FINRA is issuing this *Notice* to restate and supplement prior guidance regarding the circumstances under which a firm or individual may influence the outcome of an investigation by demonstrating extraordinary cooperation. This *Notice* incorporates FINRA's prior guidance and provides clarification and additional information about how FINRA assesses whether a potential respondent's cooperation is "extraordinary" and distinct from the level of cooperation expected of all member firms and their associated persons.

Questions concerning this *Notice* should be directed to:

- Lara Thyagarajan, Senior Vice President & Counsel to the Head of Enforcement, at (212) 858-4176 or Lara.Thyagarajan@finra.org; and
- Megan Davis, Senior Counsel, Enforcement, at (646) 315-7336 or Megan.Davis@finra.org.

Background & Discussion

FINRA recognizes extraordinary cooperation by respondents when making its enforcement determinations. In 2008, FINRA published *Regulatory Notice 08-70* to apprise industry participants of the factors FINRA considers in determining whether and how to award credit for extraordinary cooperation in a FINRA investigation. FINRA noted that the types of extraordinary cooperation by a firm or individual that could result in credit can be categorized as follows: (1) self-reporting before regulators are aware of the issue; (2) extraordinary steps to correct deficient procedures and systems; (3) extraordinary remediation to customers; and (4) providing substantial assistance to FINRA's investigation. The guidance set forth in *Regulatory Notice 08-70* is restated and incorporated into this *Notice*.

Subsequent changes to FINRA's rules, including the adoption of FINRA Rule 4530(b)—which requires member firms to report internal conclusions of violations of certain laws, rules, regulations or standards of conduct—may have created uncertainty around the continued impact that self-reporting may have on a potential respondent's ability to receive credit for extraordinary cooperation. In addition, other FINRA rules and policies—such as FINRA Rule 8210 and FINRA's *Sanction Guidelines*—expect certain levels of cooperation in every case.

To provide further clarity on the differences between required cooperation and extraordinary efforts, and in response to comments from the industry requesting further transparency,[1] FINRA is issuing this *Notice*, which incorporates its prior guidance and provides additional information regarding the circumstances under which credit for extraordinary cooperation will be awarded and the nature of credit available. In doing so, FINRA hopes to incentivize firms and associated persons to voluntarily and proactively assist FINRA. This, in turn, will aid FINRA in meeting its objectives of investor protection and market integrity by quickly identifying and remediating misconduct.

What Is Extraordinary Cooperation?

FINRA's *Sanction Guidelines* state, "Sanctions in disciplinary proceedings are intended to be remedial and to prevent the recurrence of misconduct."[2] While disciplinary actions are an important tool that FINRA uses to achieve the goals of remediation and prevention, actions taken by member firms and associated persons are also an important part of that effort. Action by member firms and associated persons that demonstrates their commitment to remediating past misconduct and preventing recurrence is essential to furthering FINRA's mission of investor protection and market integrity.

Therefore, FINRA always considers factors such as corrective measures and payment of restitution in assessing whether a disciplinary action is necessary, and, if so, what sanctions are appropriate. FINRA's *Sanction Guidelines* direct Enforcement to consider whether a respondent:

i. accepted responsibility for and acknowledged the misconduct prior to detection and intervention by the firm or a regulator;[3]

ii. voluntarily employed subsequent corrective measures, prior to detection or intervention by the firm or by a regulator, to revise general and/or specific procedures to avoid recurrence of the misconduct;[4]

iii. voluntarily and reasonably attempted, prior to detection and intervention by a regulator, to pay restitution or otherwise remedy the misconduct;[5] and

iv. provided substantial assistance to FINRA in its examination and/or investigation of the underlying misconduct.[6]

FINRA has and will continue to look to these factors when assessing sanctions in disciplinary matters.[7] For example, Enforcement may recommend a sanction that is on the low end of the specified range in the *Sanction Guidelines* based on the presence of these mitigating factors. In certain circumstances, Enforcement also may determine to forgo recommending formal disciplinary action entirely.

Enforcement may recommend a sanction that is **well below** the range set forth in the *Sanction Guidelines* or comparable precedents when respondents have voluntarily provided such material assistance to FINRA in its investigation, or effected such expedient and effective remediation, that FINRA deems these steps to constitute "extraordinary cooperation" beyond what it requires of any member firm or associated person. Member firms and associated persons who take proactive and voluntary steps well beyond those required under FINRA rules materially assist FINRA in meeting its goals of investor protection and market integrity. To recognize and incentivize such conduct, FINRA weighs these mitigating factors so heavily that the outcome of the matter is materially different than it would have been absent the respondent's extraordinary conduct.

In several matters in recent years, FINRA has granted substantial credit to firms based on their extraordinary cooperation:

- Beginning in 2015 through 2018, FINRA ordered a number of firms to pay more than $75 million in restitution, including interest, to affected customers for failing to waive mutual fund sales charges for certain charitable and retirement accounts. FINRA did not impose fines in those matters based on the firms' extraordinary cooperation. Firms initiated, prior to detection or intervention by a regulator, investigations to identify whether the misconduct existed; promptly established a plan of remediation for affected customers; promptly self-reported the conduct to FINRA; promptly took action and remedial steps to correct the violative conduct; and employed subsequent corrective measures, prior to detection or intervention by a regulator, to revise their procedures to avoid recurrence of the misconduct.

- In September 2017, FINRA ordered a respondent firm to pay approximately $9.8 million in restitution to customers who were affected by the firm's failure to establish and maintain a supervisory system reasonably designed to detect and prevent unsuitable short-term trading of unit investment trusts. While FINRA fined the firm $3.25 million, this reflected substantial credit for the firm's extraordinary cooperation and remediation to customers. The firm initiated, prior to intervention by a regulator, a firm-wide investigation to identify the scope of potentially unsuitable trades, which included the interview of a substantial number of firm personnel and the retention of an outside consultant to conduct a statistical analysis; identified harmed customers and established a plan to provide remediation; and provided substantial assistance to FINRA in its investigation.

- In October 2018, FINRA sanctioned a firm for failures to supervise firm functions it outsourced to a vendor. FINRA did not impose a fine, acknowledging, among other things, the firm's self-report, which extended beyond its obligation to self-report pursuant to FINRA Rule 4530; the extraordinary steps the firm took to remediate, including weekly meetings with the vendor's CEO and COO, hiring two full-time employees to implement controls, and assigning a dedicated manager to oversee the vendor; changing its billing structure to avoid similar issues; and conducting a comprehensive review of all its wealth management accounts to identify impacted investors, whom it voluntarily paid $4.6 million in restitution.

FINRA resolved these matters in consideration of the factors set forth in both the *Sanction Guidelines* and *Regulatory Notice 08-70*, including a consideration of both the timeliness and quality of the respondents' corrective measures and cooperation. FINRA believes these cases are good examples of its existing policy. Although the impact of extraordinary cooperation depended upon the facts and circumstances of each particular case, these matters demonstrate, among other things, that the receipt of substantial credit depended on corrective measures and cooperation aimed at broadly and quickly remediating harm.

Most recently, in January 2019, FINRA announced in *Regulatory Notice 19-04* its 529 Plan Share Class Initiative, encouraging firms to review their supervision of 529 plan sales. FINRA described common supervisory issues it had observed concerning share class recommendations and stated that it would recommend settlements with no fines for firms that choose to review their supervisory systems and procedures, self-report supervisory violations, and provide FINRA with a plan to remediate harmed customers. This initiative was announced to promote firms' compliance with the rules governing 529 plan recommendations, to promptly remedy violations, and to return money to harmed investors as quickly and efficiently as possible.

As in these prior matters, FINRA will continue to consider the factors that are set forth in the *Sanction Guidelines* and *Regulatory Notice 08-70* when determining whether credit will be given for extraordinary cooperation. Those factors are reiterated below, with additional guidance regarding how they impact FINRA's decision making:

1. Providing Credit for Steps Taken to Correct Deficient Procedures and Systems

When a firm identifies a problem involving deficient supervisory systems, procedures and controls, the firm must take corrective steps to fully remediate the problem. In considering whether to provide substantial credit for extraordinary cooperation, FINRA will consider whether a firm's steps to correct deficient systems and procedures go beyond these baseline requirements. Examples of corrective steps that may result in credit for extraordinary cooperation include:

- Engaging or conducting an independent audit or investigation that is thorough and far-reaching in scope beyond the immediate issue, with an eye toward identifying and remediating all related misconduct that may have occurred.
- Hiring independent consultants to ensure the adoption and implementation of improved supervisory systems, procedures and controls.
- Where the root cause of a violation relates to organizational weaknesses such as where a firm dedicated inadequate staff to the supervision of a particular business line, making organizational changes by, for example, creating new supervisory positions, adjusting reporting lines or, if necessary, removing or disciplining responsible individuals, including those in supervisory roles (although personnel changes are not necessarily required to achieve extraordinary cooperation).

FINRA will consider whether the firm took these or other corrective steps promptly following its discovery of the misconduct, prioritizing the remediation of any deficiencies. Additionally, FINRA will consider whether the firm maintained an open dialogue with FINRA staff regarding improvements to supervisory systems, procedures and controls, and provided FINRA with ready access and information to evaluate whether new systems, procedures and controls are reasonable.

FINRA staff will also consider the breadth of a firm's remediation. For example, if a firm identifies deficient procedures that affect a particular department or product line, the firm must review and correct the identified procedures. In contrast, FINRA may consider the firm's responses "extraordinary" when the firm conducts a broader assessment, which goes beyond the scope of the original investigation, and looks for and remediates similar deficiencies in procedures that govern other aspects of its business.

Although FINRA will, consistent with the *Sanction Guidelines*, take into consideration the timing of steps taken to correct deficient systems or procedures when deciding whether to award credit,[8] FINRA recognizes that there is some tension between expecting firms to report misconduct promptly and, at the same time, giving priority to corrective measures that a firm takes prior to detection by FINRA or other regulators (*e.g.*, prior to any self-report). For that reason, and in order to encourage the timely self-reporting of misconduct, FINRA will consider, in appropriate circumstances, giving credit for corrective measures taken promptly **after** a firm reports the misconduct.

2. Providing Credit for Restitution to Customers

FINRA's overarching mission is to protect investors and promote vibrant markets. As FINRA has previously stated, when a member firm or registered representative engages in misconduct, restitution for harmed customers is our highest priority. Therefore, if a respondent's misconduct has caused customer harm, it will be difficult for that respondent to obtain credit for extraordinary cooperation without making complete and timely restitution to injured customers.

The *Sanction Guidelines* recognize the importance of prompt restitution and treat as a mitigating factor for sanctions purposes the fact that a firm or associated person voluntarily paid restitution prior to detection or intervention by a regulator.[9] Because FINRA expects firms and associated persons to make full restitution to injured customers[10] in all cases, the mere payment of restitution will not result in credit for extraordinary cooperation. Rather, as with other corrective measures, FINRA will consider whether a firm or associated person has proactively and voluntarily taken extraordinary steps to ensure that restitution is paid as quickly as possible, in a manner that ensures all harmed customers are made whole.

This is particularly relevant in matters involving widespread, systemic failures, where identifying injured customers and calculating each individual's losses can be complex and time consuming. For example, where a firm's failure to supervise compliance with its suitability obligations has resulted in customer losses, it could review the recommendations made in each of its customer's accounts, calculate individual losses resulting from the failure to comply with the suitability duty, and pay restitution to the customers who were harmed. This complex process can take significant time. An extraordinary step, in contrast, could be one that significantly accelerates the process in order to return money to investors sooner. For example, implementing a methodology to efficiently identify customers for restitution, such as a statistical approach, could meaningfully reduce the time it would take for investors to receive restitution. Similarly, taking steps to accelerate a trade-by-trade review (such as dedicating staff members, hiring temporary help, paying for overtime, or re-prioritizing other projects) may constitute extraordinary efforts.

When assessing whether a respondent has exceeded expectations regarding restitution, FINRA will consider whether the respondent is proactive about identifying and proposing an expeditious methodology, and willing to engage in a dialogue with FINRA and other regulators about the appropriate way to identify the pool of affected customers and to calculate the amount of restitution to pay back customers as swiftly as possible.

Even where restitution is paid after FINRA becomes aware of the misconduct (for example, if the firm reports the misconduct within 30 days of discovery as required by Rule 4530), FINRA will consider whether to award credit when the restitution remediated all potential harm and was paid promptly at the initiative of the firm, prior to any order by FINRA or another regulator.

3. Self-Reporting of Violations

One reason for this updated guidance is to clarify how FINRA considers self-reporting in light of the adoption of Rule 4530. Rule 4530 replaced NASD Rule 3070 in February 2011 and, in subsection (b), unlike its predecessor, requires member firms to self-report internal conclusions regarding violations of certain laws, rules, regulations or standards of conduct. Although self-reporting of such internal conclusions was already required for NYSE member firms under NYSE Rule 351(a)(1), FINRA Rule 4530(b) represented a significant change for many firms.

As noted previously in the Rule 4530 Frequently Asked Questions, to be considered "extraordinary cooperation," self-reporting must, at a minimum, "go significantly beyond" what is required to comply with regulatory obligations.[11] Credit will not be awarded to firms merely for complying with their reporting obligations under Rule 4530. Nor will firms and associated persons be given credit for merely complying with their obligations to provide information or testimony in response to regulatory requests made pursuant to Rule 8210. If, however, a firm self-reports misconduct that does not fall within the reporting requirements of Rule 4530, then self-reporting will be considered in determining whether to award credit.

In matters where a self-report is required pursuant to Rule 4530, FINRA will consider whether the firm self-reports information beyond that which is required by the rule. For example, a firm exceeds its regulatory obligation when it proactively and voluntarily asks to meet with FINRA staff, provides summaries of key facts, and identifies and explains key documents. This type of substantial assistance is further described below.

FINRA also will consider whether the firm proactively detected the misconduct through compliance, audits or other surveillance, as opposed to identifying the misconduct only after receiving notice from customers, counterparties or regulators. FINRA also will consider whether the firm made diligent efforts to identify and inform FINRA of the relevant facts as soon as it discovered the issue, and kept FINRA updated as it learned new facts through continuing investigation.

Finally, FINRA will consider whether the firm reported the misconduct to the public and other regulators, as appropriate. FINRA also may consider the level of the firm's cooperation with other regulators and, if appropriate, law enforcement bodies, particularly in matters where multiple agencies are investigating the misconduct.[12]

4. Providing Substantial Assistance to FINRA Investigations

In addition to the above factors, FINRA also will consider giving credit to firms or associated persons for providing substantial assistance to FINRA in its investigation of the underlying misconduct.[13] In assessing whether firms have provided substantial assistance, FINRA will consider the degree of assistance that might be expected given a firm's size and resources, as well as the scope of the misconduct within the organization and the steps taken to address systemic deficiencies; there is no one-size-fits-all approach to the steps that FINRA would consider substantial assistance. Credit is potentially available to any firm or individual that cooperates substantially, including the largest broker-dealers and single-employee firms.

To constitute substantial assistance, industry participants should fully inform FINRA about the potential misconduct—including all relevant issues, products, markets and industry participants—in ways that go far beyond merely responding to requests made under Rule 8210. For example, substantial assistance deserving of credit might include:

- volunteering relevant information that the firm believes would be helpful even if FINRA did not directly request the specific documents or information;
- providing analysis of trading or other activity that assists FINRA in understanding the conduct at issue;
- volunteering facts related to the involvement of particular parties who may have committed violations;
- providing demonstrations of trading or other systems at issue;
- after identifying misconduct by an individual employee, conducting a thorough and expeditious review of the employee's misconduct and promptly sharing the findings with FINRA;
- volunteering relevant industry knowledge to help FINRA quickly assimilate information about a complex product or practice. Examples could include providing information about the considerations or issues that affect an industry-wide common practice;
- providing detailed summaries or chronologies of relevant events prior to receiving a Rule 8210 or other regulatory request;
- voluntarily assisting FINRA in obtaining effective access to firm offices, records or computer systems prior to receiving a Rule 8210 or other regulatory request;
- identifying witnesses who possess relevant information, including witnesses over whom FINRA lacks jurisdiction, and making those witnesses available for interviews; and
- conducting a thorough and independent audit or investigation, using counsel or consultants where appropriate, and fully disclosing the findings to FINRA.[14]

What Type of Credit Will Be Given in Return for Extraordinary Cooperation?

When FINRA determines that a firm should be given credit for extraordinary cooperation, that credit may take many forms. For example, where a problem has been fully remediated, FINRA often concludes that no enforcement action is warranted and closes an investigation with no further action or with a Cautionary Action Letter.

In other cases, FINRA might determine that an enforcement action is appropriate to remedy or prevent harm, even where a firm has provided extraordinary cooperation. In those matters, FINRA may provide credit by reducing the sanctions imposed. When credit is given in the form of a reduced fine, the reduction normally will be substantial. Indeed, in appropriate cases, as illustrated in several of the examples above, FINRA may consider imposing formal discipline without any fine. FINRA also may give credit by declining to require an undertaking. For example, FINRA may forego requiring a firm to hire an independent consultant where, although a systemic deficiency is in an extended period of remediation, the firm is taking other extraordinary steps to address the problem.

How Does FINRA Plan To Be More Transparent About Credit for Extraordinary Cooperation?

In each case where the applicable principal considerations and the factors set forth in this *Regulatory Notice* result in a respondent receiving credit for extraordinary cooperation, FINRA will include in the Letter of Acceptance, Waiver and Consent (AWC) memorializing the settlement a new section titled, "Credit for Extraordinary Cooperation." FINRA will describe the factors that resulted in credit being given, as well as the type of credit.

In order to provide more useful guidance to the industry, FINRA will take additional steps to distribute information about instances when it has deemed cooperation to be extraordinary, in ways that are more accessible and easier to identify. For example, FINRA occasionally issues press releases in connection with individual cases to highlight matters deemed worthy of public attention.[15] In press releases, FINRA will note factors that led the respondent to receive credit, as well as the type of credit. Similarly, when FINRA proceeds without formal action in connection with an investigation, traditionally FINRA has not made public a statement regarding the action. Going forward, when FINRA gives credit for extraordinary cooperation that results in FINRA electing to proceed without formal action, FINRA will determine, on a case-by-case basis, whether it would be useful to provide additional transparency regarding the factors that led to FINRA's decision and, when appropriate, publish information about those individual cases. Unless the firm or associated person gives permission to be named, FINRA will preserve their anonymity by describing the respondents' extraordinary cooperation at a sufficiently high level to shield their identities.

FINRA also seeks to provide clear guidance on the difference between matters characterized by extraordinary cooperation, and matters in which the respondent's conduct did not exceed its regulatory obligations but sanctions determinations were materially affected by other considerations. As described above, FINRA always considers factors such as corrective measures and payment of restitution in assessing whether a disciplinary action is necessary and what sanctions are appropriate. For example, the Principal Considerations in the *Sanction Guidelines* include "Whether the respondent voluntarily and reasonably attempted, prior to detection and intervention, to pay restitution or otherwise remedy the misconduct." Accordingly, Enforcement may consider a firm's voluntary payment of restitution to be mitigating and recommend a sanction on the low end of the specified range in the Sanction Guidelines. In contrast, Enforcement may consider it "extraordinary" if a firm takes significant steps to effect speedy restitution, such as re-prioritizing other projects or developing a rules-based approach to accelerate the process. Under those circumstances, FINRA may consider these additional steps so extraordinary that it recommends a sanction well below the *Sanction Guidelines* or other similar cases.

At other times, the presence of aggravating factors may materially affect the sanction determination. For example, even if a respondent remediates the problem and makes restitution as expected, FINRA may recommend a more severe sanction due to aggravating factors in the matter, such as prior disciplinary history;[16] the nature of the underlying misconduct, including whether the misconduct was intentional or reckless,[17] involved numerous acts or a pattern of misconduct, and continued over an extended period of time;[18] the nature and extent of injury to the investing public, a member firm and other market participants;[19] whether the respondent profited from the misconduct;[20] and whether the respondent engaged in the misconduct notwithstanding prior warnings from FINRA, another regulator or a supervisor.[21]

In general, the factual findings set forth in an AWC should always include any facts that were considered as aggravating or mitigating for sanctions purposes. However, where appropriate an AWC may also include a new section titled, "Sanctions Considerations." In that section, FINRA may identify mitigating or aggravating factors (such as those discussed in the relevant Principal Considerations from the *Sanction Guidelines*) that affected FINRA's sanction determination.

Can Individuals Also Receive Credit for Extraordinary Cooperation?

Credit for extraordinary corrective measures and cooperation is available to individuals as well as firms. FINRA believes many of the principles discussed above may apply equally to individuals. For example, although individuals may not be able to correct deficient firm procedures and systems, they may still self-report misconduct, provide substantial assistance during an investigation, and pay restitution to customers with appropriate notice to and involvement by a member firm. However, the presence of aggravating factors may weigh against credit for extraordinary cooperation, and certain aggravating factors

are more likely to be present in cases involving individuals, such as intentional or reckless misconduct,[22] attempts to conceal misconduct from a member firm,[23] and misconduct notwithstanding prior warnings from a supervisor.[24]

In evaluating whether to give credit to an individual, FINRA also will consider the same four general factors outlined in the SEC's policy regarding cooperation by individuals: (1) the assistance provided by the individual; (2) the importance of the underlying matter in which the individual cooperated; (3) the societal interest in holding the individual accountable for his or her misconduct; and (4) the appropriateness of credit based upon the profile of the cooperating individual.[25]

Endnotes

1. *See* May 8, 2017, letter from the Securities Industry and Financial Markets Association to FINRA in response to Special Notice – Engagement Initiative (Mar. 21, 2017), at 8 (urging FINRA to, among other things, "publicize when good credit is given").
2. *Sanction Guidelines* (March 2019 version), at 3.
3. Principal Consideration No. 2.
4. Principal Consideration No. 3.
5. Principal Consideration No. 4.
6. Principal Consideration No. 12.
7. As was the case with *Regulatory Notice 08-70*, this *Notice* is intended to provide the industry with additional guidance concerning the factors that FINRA considers in assessing whether formal discipline is warranted and, if so, the appropriate sanctions in the context of settlement discussions prior to initiation of a disciplinary proceeding. Nothing herein is intended to alter the *Sanction Guidelines*, FINRA rules or other applicable requirements.
8. *See* Principal Consideration No. 3 (treating as a mitigating factor corrective measures taken "prior to detection or intervention" by a regulator).
9. Principal Consideration No. 4.
10. FINRA reminds associated persons that paying restitution or otherwise settling a customer complaint without notice to the firm is a violation of FINRA Rule 2010, and can result in sanctions of up to two years or, in egregious cases, a bar. *Sanction Guidelines*, at 34.
11. *Regulatory Notice 11-32*, A6.
12. *Cf.* General Principles Applicable to All Sanction Determinations, No. 7 (directing adjudicators to consider, where appropriate, sanctions previously imposed by other regulators for the same conduct).
13. Principal Consideration No. 12.
14. Nothing has changed about FINRA's approach with respect to attorney-client privilege. The waiver or non-waiver of privilege itself will not be considered in connection with granting credit for cooperation. *See* endnote 9 in *Regulatory Notice 08-70*.

15. *See www.finra.org/newsroom/newsreleases*.
16. Principal Consideration No. 1.
17. Principal Consideration No. 13.
18. Principal Consideration Nos. 8, 9.
19. Principal Consideration No. 11.
20. Principal Consideration No. 16.
21. Principal Consideration No. 14.
22. Principal Consideration No. 13.
23. Principal Consideration No. 10.
24. Principal Consideration No. 14.
25. SEC Policy Statement Concerning Cooperation by Individuals in its Investigations and Related Enforcement Actions, Release No. 34-61340, 17 CFR Part 202 (Jan. 19, 2010).

Regulatory Notice 22-10

Supervision

FINRA Reminds Member Firms of the Scope of FINRA Rule 3110 as it Pertains to the Potential Liability of Chief Compliance Officers for Failure to Discharge Designated Supervisory Responsibilities

Summary

Chief Compliance Officers (CCOs) at member firms play a vital role. For example, CCOs and their compliance teams help design and implement compliance programs, help educate and train firm personnel, and work in tandem with senior business management and legal departments to foster compliance with regulatory requirements. In this way, CCOs help promote strong compliance practices that protect investors and market integrity, as well as the member firm itself.[1]

Rule 3110 (Supervision) imposes specific supervisory obligations on member firms.[2] The responsibility to meet these obligations rests with a firm's business management, not its compliance officials. The CCO's role, in and of itself, is advisory, not supervisory. Accordingly, FINRA will look first to a member firm's senior business management and supervisors to determine responsibility for a failure to reasonably supervise. FINRA will not bring an action against a CCO under Rule 3110 for failure to supervise except when the firm conferred upon the CCO supervisory responsibilities and the CCO then failed to discharge those responsibilities in a reasonable manner.[3] As a result, charges against CCOs for supervisory failures represent a small fraction of the enforcement actions involving supervision that FINRA brings each year.[4]

Questions regarding this *Notice* should be directed to:

- Christopher Perrin, Counsel to the Head of Enforcement, Enforcement, at (415) 217-1121 or christopher.perrin@finra.org; and
- Philip Shaikun, Vice President and Associate General Counsel, Office of General Counsel, at (202) 728-8451 or Philip.Shaikun@finra.org.

March 17, 2022

Notice Type
- Reminder

Suggested Routing
- Compliance
- Legal
- Senior Management

Key Topics
- Compliance
- Supervision

Referenced Rules & Notices
- FINRA Rule 0140
- FINRA Rule 1220
- FINRA Rule 3110
- FINRA Rule 3130
- FINRA Rule 3310
- Notice to Members 99-45
- Notice to Members 01-51
- Regulatory Notice 18-15

Background and Discussion

I. THE SCOPE OF RULE 3110 REGARDING INDIVIDUAL LIABILITY

Rule 3110 sets out a comprehensive set of supervisory obligations for member firms and requires firms to designate individual supervisors and identify their responsibilities. The rule requires each member firm to establish and maintain a system, including written procedures, to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules.[5] The rule also requires each member firm to designate an appropriately registered principal or principals with authority to carry out the supervisory responsibilities of the member for each type of broker-dealer business in which it engages, to designate one or more appropriately registered principals in branch offices with authority to carry out the supervisory responsibilities assigned to that office, and to assign each registered representative to an appropriately registered person who is responsible for supervising that representative's activities.[6] Individual liability under Rule 3110 is predicated upon the firm's express or implied designation of supervisory personnel and the delegation of supervisory responsibility to the designated individuals.[7] Individual supervisors have an additional duty under Rule 3110 to investigate "red flags" that suggest misconduct at the firm may be occurring and to act reasonably upon the results of the investigation.[8] FINRA can bring enforcement actions under Rule 3110 against individual supervisors when they fail to discharge reasonably their supervisory responsibilities.[9]

A firm's supervisory obligations under Rule 3110 rest with the firm and its president (or equivalent officer or individual, *e.g.,* CEO) and flow down by delegation to the firm's designated supervisors.[10] The firm's president (or equivalent officer or individual), not its CCO, "bears ultimate responsibility for compliance with all applicable requirements unless and until he [or she] reasonably delegates particular functions to another person in that firm, and neither knows nor has reason to know that such person's performance is deficient."[11] Accordingly, the president (or equivalent officer or individual) and designated principals are responsible for fulfilling the firm's supervisory obligations under Rule 3110.

II. THE ROLE OF A CCO WITHIN A MEMBER FIRM

A CCO's role at a member firm, by contrast, is advisory, not supervisory. FINRA recognizes that compliance and supervision are separate, if related, functions. In *Notice to Members 99-45*, FINRA stated that "[i]t is important [to] recognize the distinction between written compliance guidelines and written supervisory procedures."[12] A CCO and the compliance team is, in the normal course, responsible for the former, not the latter. "Compliance guidelines generally set forth the

applicable rules and policies that must be adhered to and describe specific practices that are prohibited."[13] By contrast, written supervisory procedures document the supervisory system to ensure that compliance guidelines are being followed.

To fulfill the compliance function, FINRA requires firms to designate one or more appropriately registered principals as a CCO.[14] As set forth in FINRA Rule 3130, Supplementary Material .05, "A [CCO] is a primary advisor to the member on its overall compliance scheme and the particularized rules, policies and procedures that the member adopts."[15] Neither Rule 3110 nor Rule 3130, by themselves, attach supervisory responsibilities to a CCO.[16]

A CCO can and often does occupy another position at a firm, such as CEO.[17] In such circumstances, CCOs likely would fall within the scope of Rule 3110 because of the supervisory authority designated to them based on another non-CCO position they hold within a firm's business management. When an individual's sole position at a firm is that of CCO, a more extensive assessment of liability under Rule 3110 may be needed, as outlined in the following section.

III. ASSESSING LIABILITY UNDER RULE 3110 AGAINST A CCO

A. Designation of Supervisory Responsibility

A CCO is not subject to liability under Rule 3110 because of the CCO's title or because the CCO has a compliance function at a member firm. A CCO will be subject to liability under Rule 3110 only when—either through the firm's written supervisory procedures or otherwise—the firm designates the CCO as having supervisory responsibility. This designation can occur in several ways. First, the member's written procedures might assign to the CCO the responsibility to establish, maintain and update written supervisory procedures, both generally as well as in specific areas (*e.g.,* electronic communications). Second, the written procedures might assign to the CCO responsibility for enforcing the member's written supervisory procedures or other specific oversight duties usually reserved for line supervisors. Third, apart from the written procedures, a member firm, through its president or some other senior business manager, might also expressly or impliedly designate the CCO as having specific supervisory responsibilities on an ad hoc basis. Or the CCO may be asked to take on specific supervisory responsibilities as exigencies demand, such as the review of trading activity in customer accounts or oversight of associated persons. Only in circumstances when a firm has expressly or impliedly designated its CCO as having supervisory responsibility will FINRA bring an enforcement action against a CCO for supervisory deficiencies.

B. Applying the Reasonableness Standard

Even when a CCO has been designated as having supervisory responsibilities, FINRA will bring an action under Rule 3110 against the CCO only if the CCO has failed to discharge those responsibilities in a reasonable manner—as it would with any individual who has supervisory responsibility. Accordingly, once FINRA has found that the CCO has been designated by the firm as having supervisory responsibilities—including responsibility for establishing, maintaining and enforcing the firm's written supervisory procedures that are reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules—the next question is whether the CCO reasonably discharged his or her designated supervisory responsibilities.

For example, if the CCO is responsible for establishing, maintaining and enforcing the firm's written supervisory procedures, FINRA will ask whether the procedures were reasonably tailored to the firm's business and whether they addressed the specific activities of the firm's personnel. Whether a CCO's performance of these responsibilities was reasonable depends upon the facts and circumstances of a particular situation. When assessing potential liability under Rule 3110, FINRA will evaluate whether the CCO's conduct in performing designated supervisory responsibilities was reasonable in terms of achieving compliance with the federal securities laws, regulations, or FINRA rules.

C. Factors For and Against Charging a CCO under Rule 3110

Not every violation of a FINRA rule results in a formal disciplinary action, so even when FINRA finds that a CCO failed to reasonably perform a designated supervisory responsibility, FINRA will consider whether charging the CCO under Rule 3110 in a formal disciplinary action is the appropriate regulatory response to address the violation. Factors that might weigh in favor of charging a CCO are the same factors that could apply to any individual who has supervisory responsibility under Rule 3110 and include, but are not limited to, the following: (1) the CCO was aware of multiple red flags or actual misconduct and failed to take steps to address them;[18] (2) the CCO failed to establish, maintain, or enforce a firm's written procedures as they related to the firm's line of business;[19] (3) the CCO's supervisory failure resulted in violative conduct (*e.g.,* a CCO who was designated with responsibility for conducting due diligence failed to do so reasonably on a private offering, resulting in the firm lacking a reasonable basis to recommend the offering to its customers);[20] and (4) whether that violative conduct caused or created a high likelihood of customer harm.[21]

Factors that might weigh against charging the CCO include, but are not limited to, the following: (1) the CCO was given insufficient support in terms of staffing, budget, training, or otherwise to reasonably fulfill his or her designated supervisory responsibilities;[22] (2) the CCO was unduly burdened in light of competing functions and responsibilities;[23] (3) the CCO's supervisory responsibilities, once designated, were poorly defined, or shared by others in a confusing or overlapping way;[24] (4) the firm joined with a new company, adopted a new business line, or made new hires, such that it would be appropriate to allow the CCO a reasonable time to update the firm's systems and procedures; and (5) the CCO attempted in good faith to reasonably discharge his or her designated supervisory responsibilities by, among other things, escalating to firm leadership when any of (1)–(4) were occurring.[25]

In addition to the above factors, FINRA also will consider whether it is more appropriate to charge the firm or its president with failure to reasonably supervise rather than the CCO. Likewise, FINRA will consider whether it is more appropriate to charge another individual at the firm, such as an executive manager or a business line supervisor, who had more direct responsibility for the supervisory task at issue, or who was more directly involved in the supervisory deficiency. Finally, FINRA also will consider whether, based on the facts and circumstances of a particular case, it is more appropriate to bring informal, as opposed to formal, action against the CCO for failure to supervise. In some cases, it may be more appropriate to issue a Cautionary Action Letter, particularly in cases involving a CCO's first-time violation of Rule 3110.

Endnotes

1. *See also* FINRA Rule 3130, Supplementary Material .05 (Role of the Chief Compliance Officer).

2. This *Notice* is limited to FINRA Rule 3110. It does not address other supervisory requirements under federal securities laws. *Cf.* SEC, Division of Trading and Markets, Frequently Asked Questions about Liability of Compliance and Legal Personnel at Broker-Dealers under Sections 15(b)(4) and 15(b)(6) of the Exchange Act, Sept. 30, 2013; *Compliance Programs of Investment Companies and Investment Advisers*, Release Nos. IA-2204, IC-26299, 2003 SEC LEXIS 2980, at n.73 (Dec. 17, 2003) (discussing when a CCO might be subject to Section 203(e)(6) of the Investment Advisers Act of 1940).

3. This *Notice* focuses on CCOs and does not encompass anti-money laundering compliance personnel. *See* FINRA Rule 3310(d); Rule 3310, Supplementary Material .02 (Review of Anti-Money Laundering Compliance Person Information). It also does not address enforcement actions against CCOs for misconduct unrelated to designated supervisory responsibilities, such as providing false documents to FINRA or failing to timely update their Uniform Application for Securities Industry Registration or Transfer (Form U4). *See, e.g., Merrimac Corporate Securities, Inc.*, Exchange Act Release No. 86404, 2019 SEC LEXIS 1771, at *9 (July 17, 2019); *Allen Holeman*, Exchange Act Release No. 86523, 2019 SEC LEXIS 1903, at *16-17 (July 31, 2019).

4. For example, from 2018–2021, of the nearly 440 FINRA enforcement actions involving violations of Rule 3110 for supervisory failures, CCOs were charged in only 28 instances. And in only 10 of these matters did FINRA charge a CCO who was not also the chief executive officer (CEO) or president of the firm. For each of these 10 matters, FINRA found that the firm had conferred upon the CCO specific supervisory responsibilities which the CCO failed reasonably to perform, in violation of Rule 3110.

5. *See* Rules 3110(a) and (b). Rule 3110 applies to persons associated with a member firm as much as it applies to a member firm. *See* FINRA Rule 0140(a) ("Persons associated with a member shall have the same duties and obligations as a member under the Rules."). Thus, FINRA may bring an action against an associated person, including a CCO, when FINRA finds the individual has violated Rule 3110.

6. *See* Rules 3110(a)(2), (4) and (5). Rule 3110(b)(6)(A) requires a firm's written supervisory procedures to include "the titles, registration status, and locations of the required supervisory personnel and the responsibilities of each supervisory person."

7. Importantly, to bring a case under Rule 3110, FINRA does not have to establish an underlying violation of the federal securities laws or other FINRA rules. *Dep't of Enforcement v. Lek Securities Corp.,* No. 2009020941801, 2016 FINRA Discip. LEXIS 63, at *35-36 (NAC Oct. 11, 2016).

8. *Ronald Pelligrino*, Exchange Act Release No. 59125, 2008 SEC LEXIS 2843, at *33 (Dec. 19, 2008) ("'Once indications of irregularities arise, supervisors must respond appropriately.'") (*quoting La Jolla Capital Corp.*, 54 S.E.C. 275, 285 (1999)). *See also Regulatory Notice 18-15* (April 2018) ("Member firms should be reviewing and updating their supervisory systems and procedures for hiring practices, monitoring brokers and investigating red flags suggestive of misconduct.")

9. *See, e.g., Dep't of Enforcement v. Clements,* No. 2015044960501, 2018 FINRA Discip. LEXIS 11, at *50 (NAC May 17, 2018) (supervisor should have "discharged [his] responsibilities reasonably").

10. *See Wedbush Securities, Inc.,* Exchange Act Release No. 78568, 2016 SEC LEXIS 2794, at *34 (Aug. 12, 2016).

11. *Id.* at *29 (quotation marks omitted). *See also John B. Busacca, III,* Exchange Act Release No. 63312, 2010 SEC LEXIS 3787, at *37-38 (Nov. 12, 2010) (finding that the president's supervision was deficient during the period that he assumed overall responsibility for the firm's operations and did not delegate this responsibility).

12. *Notice to Members 99-45* (June 1999).

13. *Id.*

14. *See also* FINRA Rule 1220(a)(3) (Compliance Officer).

15. Rule 3130, Supplementary Material .05.

16. *See Notice to Members 01-51* (August 2001) ("The chief compliance officer registration requirement does not create the presumption that a chief compliance officer has supervisory responsibilities or is otherwise a control person. As in the past, NASD Regulation will hold a chief compliance officer responsible for supervision only where supervision is his or her responsibility. Many chief compliance officers are already registered as principals. NASD Regulation does not presume that these individuals have supervisory responsibility by virtue of their title. NASD Regulation will continue to determine whether a chief compliance officer is acting in a supervisory capacity based on the actual responsibilities and functions that the chief compliance officer performs for the firm."). *See also* Rule 3130, Supplementary Material .07 (Certification of Business Line Responsibility) ("The FINRA Board of Governors recognizes that supervisors with business line responsibility are accountable for the discharge of a member's compliance policies and written supervisory procedures. The signatory to the certification is certifying only as to having processes in place to establish, maintain, review, test and modify the member's written compliance and supervisory policies and procedures and the execution of this certification and any consultation rendered in connection with such certification does not by itself establish business line responsibility.").

17. *See* Rule 3130, Supplementary Material .08 (Ability of Chief Compliance Officer to Hold Other Positions). *See also* note 4.

18. *Dep't of Enforcement v. Cantone Research, Inc.,* No. 2013035130101, 2019 FINRA Discip. LEXIS 5, at *99-100 (NAC Jan. 16, 2019) (finding that firm designated its CCO, who also had the title of Vice President, as a supervisor of registered representatives and that the CCO was "aware of numerous red flags," failed to address the red flags, and therefore failed to discharge supervisory obligations); *Dep't of Enforcement v. Fox Financial Management Corp.,* No. 2012030724101, 2017 FINRA Discip. LEXIS 3, at *17-18 (NAC Jan. 6, 2017).

19. *See Merrimac,* 2019 SEC LEXIS 1771 at *80-84 (finding a CCO liable for his failure "in any meaningful way to develop the procedures that FINRA's rules required" for a line of business at the firm); see also *Ryan Carlson et al.,* Letter of Acceptance, Waiver, and Consent (FINRA Case No. 2018060267902) (Mar. 29, 2021).

20. *Matthew Bahrenburg,* Letter of Acceptance, Waiver, and Consent (FINRA Case No. 2018057457101) (Aug. 24, 2020).

21. *Id.*

22. *Thaddeus North,* Exchange Act Release No. 84500, 2018 SEC LEXIS 3001, at *34-35 (Oct. 29, 2018), *aff'd,* 828 F. App'x 729 (D.C. Cir. 2020).

23. *Id.* at *28-29 ("[The Commission] found a compliance director's failure to respond to NASD's requests for information mitigated by the 'extraordinary demands on the compliance group' during the relevant time.").

24. *Id.* at *28 ("[The Commission has] dismissed proceedings against an individual with compliance responsibilities that alleged liability for causing his firm's violations of the securities laws where another official at the firm had responsibility for overseeing the relevant activities and the respondent was never asked to evaluate the relevant regulatory issues.").

25. *Id.* ("[The Commission has] dismissed proceedings alleging supervisory failures where the respondent conducted his own independent investigation in response to indications of wrongdoing and recommended responsive action."); *Merrimac,* 2019 SEC LEXIS 1771, at *73 (liability should not attach "where a CCO made a reasonable inquiry and determined erroneously that no further action needed to be taken in light of that inquiry").

2022 Annual Conference

May 16 –18 | Washington, DC | Hybrid Event

Financial and Operational Effective Practices

Tuesday, May 17, 2022
11:00 a.m. – 12:00 p.m.

This session provides an overview of current financial and operational topics and recent developments in financial and operational rules and requirements applicable to broker-dealers. Join FINRA staff and industry practitioners as they discuss current financial and operational risks and issues impacting firms as well as new and proposed rules. Attendees also learn effective practices taken by compliance and risk professionals to monitor financial and operational risks.

Moderator:

Kris Dailey
Vice President, Regulatory Development Services
FINRA Office of Financial and Operational Risk Policy

Panelists:

Ann Duguid
Senior Director
FINRA Office of Financial and Operational Risk Policy

Brian Kowalski
Senior Director, Diversified Risk Monitoring
FINRA Member Supervision

Michael Lyons
Chief Financial Officer and Treasurer
National Financial Services

Michael Macchiaroli
Associate Director, Office of Broker-Dealer Finances, Division of Trading and Markets
U.S. Securities and Exchange Commission (SEC)

Financial and Operational Effective Practices Panelists Bios:

Moderator:

Kris Dailey is Vice President in FINRA's Office of Financial and Operational Risk Policy. Ms. Dailey is responsible for leading a team of professionals in developing and interpreting rules and providing policy advice to FINRA staff and member firms. Ms. Dailey's responsibilities span throughout several areas including broker-dealer net capital, liquidity management, accounting and financial reporting obligations, recordkeeping requirements, customer protection requirements, margin requirements and securities clearance and settlement operations, including prime brokerage and financing arrangements. Ms. Dailey's prior roles at FINRA included responsibility for the development of an automated data collection and analysis program in support of FINRA's financial and operational examinations of member firms, assessments of firms' quantitative market and credit risk measurement methodologies and new and continuing membership applications. Before joining FINRA, Ms. Dailey spent more than 15 years at NYSE Regulation, in staff and managerial positions responsible for the examinations and ongoing monitoring of member firms' financial and operational condition. Ms. Dailey received a B.S. in Finance from St. John's University and a M.B.A. from Fordham University.

Panelists:

Ann Duguid is Senior Director in the Office of Financial and Operational Risk Policy. In this role, she works closely with FINRA's Member Supervision team providing both accounting policy and financial and operational interpretive guidance related to both introducing and clearing broker dealers. Prior to joining FINRA, Mrs. Duguid worked at J.P. Morgan & Co., where she held various positions, including legal entity controller of J.P. Morgan Securities LLC., regulatory reporting manager (SEA 15c3-1, 15c3-3 and CFTC regulatory reporting), line of business controller for U.S. futures and options clearing and global OTC derivatives brokerage businesses. A Certified Public Accountant with more than 25 years of experience, Ms. Duguid began her career as an auditor at Arthur Andersen & Co. She holds a BBA in Accounting and Management Information Systems from Loyola College in Baltimore, MD.

Brian Kowalski is Senior Director and Single Point of Accountability (SPoA) of Risk Monitoring for the Diversified Firm Group within FINRA's Member Supervision Department. In his role, Mr. Kowalski provides strategic leadership and oversees the teams responsible for ongoing risk assessment and monitoring of Medium Diversified firms. He and his team are also responsible for coordination with Examination Program Management on the strategy and execution of related examinations. Prior to this role, Mr. Kowalski was a Surveillance Director within the Risk Oversight and Operational Regulation group of Member Supervision. Mr. Kowalski joined FINRA in 2010 after spending nine years at National Financial Services, LLC in various operations and regulatory control functions.

Michael Lyons is Chief Financial Officer and Treasurer of Fidelity's National Financial Services and other Fidelity Brokerage companies. He is co-chair of the FINRA Financial Responsibility Committee, Chair Emeritus of the SIFMA Financial Management Society and a member of the SIFMA Capital and Margin Forum. Mr. Lyons oversees the regulatory and treasury functions for all of Fidelity's broker dealers. Mr. Lyons has been with Fidelity for 16 years and served in various capacities including CFO of Capital Markets and the Operations business units. He also serves as an active member of various not for profit boards and a speaker at various industry conferences. Prior to joining Fidelity, Mr. Lyons was a partner at BDO Seidman in the Financial Services group. He was previously Chief Administrative Officer of U.S. Clearing, a subsidiary of the Quick and Reilly Group, and a Senior Manager at Arthur Andersen. Mr. Lyons earned a BS in Accounting from St. John's University. Mr. Lyons is a CPA and holds Series 27 and 99 licenses.

Michael A. Macchiaroli is Associate Director of the Office of Broker-Dealer Finances, Division of Trading and Markets for the U.S. Securities and Exchange Commission. He is responsible for the broker-dealer financial responsibility program, which deals with the capital record-keeping, reporting and customer protection Rules. Mr. Macchiaroli has been employed at the Commission since 1970 and in the Division of Trading and Markets since 1978.

Financial and Operational Effective Practices

Panelists

- **Moderator**
  - Kris Dailey, Vice President, Regulatory Development Services, FINRA FINRA Office of Financial and Operational Risk Policy
- **Panelists**
  - Ann Duguid, Senior Director, FINRA Office of Financial and Operational Risk Policy
  - Brian Kowalski, Senior Director, Diversified Risk Monitoring, FINRA Member Supervision
  - Michael Lyons, Chief Financial Officer and Treasurer, National Financial Services
  - Michael Macchiaroli, Associate Director, Office of Broker-Dealer Finances, Division of Trading and Markets, U.S. Securities and Exchange Commission (SEC)

Information Notice

Redesigned eFOCUS System and SEC Security-Based Swap Reporting Requirements; Revised Supplemental Inventory Schedule

June 3, 2021

Summary

In 2019, the Securities and Exchange Commission (SEC) adopted amendments[1] that revise certain of the Financial and Operational Combined Uniform Single (FOCUS) reporting and annual report requirements that apply to brokers and dealers pursuant to SEA Rule 17a-5[2] to take account of security-based swap (SBS) activity. Further, as a result of these changes, to avoid duplication with the SEC's new requirements, FINRA has revised[3] the Supplemental Inventory Schedule (SIS) so that members that file the new FOCUS Report Part II, pursuant to the SEC's amendments, will no longer need to file the SIS. The SEC's new FOCUS reporting requirements, and the revised SIS, will apply beginning with FOCUS reports and SIS filings that report on the period ending October 31, 2021 and are required to be filed in November 2021. This *Notice* provides highlights of the upcoming changes.

Additionally, FINRA has redesigned its eFOCUS filing system to add certain enhancements and features to improve members' filing experience. Members that are quarterly filers may access the new system on FINRA Gateway beginning June 24, 2021. The new system will be made available to monthly filers beginning in July 2021.

Questions concerning this *Notice* may be directed to:

- Ann Duguid, Senior Director, Office of Financial and Operational Risk Policy, at (646) 315-8434 or Ann.Duguid@finra.org; or
- Jay Koutros, Senior Director, Member Supervision, at (646) 315-8509 or Demetrios.Koutros@finra.org.

Suggested Routing

- Compliance
- Legal
- Operations
- Regulatory Reporting
- Senior Management

Key Topic(s)

- Annual Report Filings
- FOCUS Report Filings
- Supplemental Inventory Schedule

Referenced Rules and Notices

- SEA Rule 17a-5
- Information Notice 11/23/20
- Regulatory Notice 18-38

Background

In 2019, the SEC, as part of its rulemakings pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act[4] to establish a regulatory framework for SBS, has adopted amendments to the FOCUS reporting and annual report requirements that apply to brokers and dealers. The amendments are designed, among other things, to elicit more detailed information about derivatives positions and exposures. Below are some highlights of how the SEC's amendments impact financial reporting:

- The SEC has amended FOCUS Report Part II. Members that currently file FOCUS Report Part II will file the amended FOCUS Report Part II;
- FOCUS Report Part II CSE will be discontinued. Firms that currently file FOCUS Report Part II CSE will instead file FOCUS Report Part II, as amended;[5]
- Schedule 1 (Aggregate Securities, Commodities and Swaps Positions) of FOCUS Report Part II, as amended, elicits substantially all the information that the current SIS requires. To avoid duplication with Schedule 1 of the SEC's amended FOCUS Report Part II, FINRA has revised the SIS so that members that file FOCUS Report Part II, as amended, will not need to file the SIS;
- The SEC has updated the Facing Page and Oath or Affirmation (Part III of Form X-17A-5), which members submit with their annual reports pursuant to Rule 17a-5. All members will use the amended Facing Page and Oath or Affirmation;
- FOCUS Report Part IIA is unchanged.

The SEC's new FOCUS reporting requirements, and the revised SIS, will apply beginning with FOCUS reports and SIS filings that report on the period ending October 31, 2021 and are required to be filed in November 2021.[6]

Additionally, to improve members' filing experience, FINRA is making available a redesigned eFOCUS system. Members that are quarterly filers may access the new system on FINRA Gateway beginning June 24, 2021. The new system will be made available to monthly filers beginning in July 2021. Members may visit FINRA's eFOCUS page for further information about user support and logging in to the redesigned eFOCUS system. Members with questions about the eFOCUS system may contact the Help Desk at (800) 321-6273.

Endnotes

1. *See* Securities Exchange Act Release No. 87005 (September 19, 2019), 84 FR 68550 (December 16, 2019) (Final Rule: Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security-Based Swap Participants, and Broker-Dealers) (referred to as the "Reporting Requirements Release").

2. Rule 17a-5 governs financial and operational reporting by brokers and dealers. Members are required to file with FINRA, through the eFOCUS System, reports concerning their financial and operational status using SEC Form X-17A-5 (the "FOCUS Report"). *See, e.g.,* Information Notice 11/23/20 (2021 and First Quarter of 2022 Report Filing Due Dates); *Regulatory Notice 18-38* (November 2018) (Amendments to the SEC's Financial Reporting Requirements – eFOCUS System Updates and Annual Audit Requirements).

3. See SR-FINRA-2021-013.

4. Pub. L. No. 111-203, 124 Stat. 1376 (2010).

5. Pursuant to the SEC's rulemaking, stand-alone security-based swap dealers (SBSDs) and stand-alone major security-based swap participants (MSBSPs) (that is, SBSDs and MSBSPs that are not broker-dealers and that do not have a prudential regulator) will also file FOCUS Report Part II, as amended. Separately, bank SBSDs and bank MSBSPs (that is, SBSDs and MSBSPs for which there is a prudential regulator) will file new FOCUS Report Part IIC. The SEC, by Order, has designated FINRA as the organization with which stand-alone SBSDs and stand-alone MSBSPs, and bank SBSDs and bank MSBSPs, must file FOCUS Report Part II, as amended, and FOCUS Report Part IIC, respectively. *See* Securities Exchange Act Release No. 88866 (May 14, 2020) (Order Designating Financial Industry Regulatory Authority, Inc., to Receive Form X-17A-5 (FOCUS Report) from Certain Security-Based Swap Dealers and Major Security-Based Swap Participants).

6. This broadly aligns with the October 6, 2021, "compliance date" that the SEC has set for many of its key SBS-related requirements. *See* the Reporting Requirements Release, note 1; *see also* Key Dates for Registration of Security-Based Swap Dealers and Major Security-Based Swap Participants, available on the Commission website.

Regulatory Notice 21-27

SEC Financial Responsibility Rules

FINRA Announces Update of the Interpretations of Financial and Operational Rules

July 22, 2021

Notice Type

- Guidance

Suggested Routing

- Compliance
- Finance
- Legal
- Operations
- Regulatory Reporting
- Senior Management

Key Topics

- Customer Protection
- Net Capital

Referenced Rules & Notices

- SEA Rule 15c3-1
- SEA Rule 15c3-3

Executive Summary

FINRA is making available updates to interpretations in the Interpretations of Financial and Operational Rules that have been communicated to FINRA by the staff of the SEC's Division of Trading and Markets (SEC staff). The updated interpretations are with respect to Securities Exchange Act (SEA) Rules 15c3-1 and 15c3-3.

Questions concerning this *Notice* should be directed to:

- Yui Chan, Senior Director, Office of Financial & Operational Risk Policy (OFORP), at (646) 315-8426 or Yui.Chan@finra.org;
- Ann Duguid, Senior Director, OFORP, at (646) 315-7260 or Ann.Duguid@finra.org; or
- Kathryn Mahoney, Senior Director, OFORP, at (646) 315-8428 or Kathryn.Mahoney@finra.org.

Background & Discussion

FINRA is updating interpretations in the Interpretations of Financial and Operational Rules related to SEA Rules 15c3-1 and 15c3-3, as set forth below. Page references are to the hardcopy version. These interpretations are being updated with specific additions, revisions and rescissions.

The following interpretations have been **added**:

- SEA Rule 15c3-1(c)(1)(i)/02 (Indebtedness in the Proprietary Trading Account of a Broker-Dealer) on page 182
- SEA Rule 15c3-1(c)(2)(i)(G)/01 (Services Arrangement with a Parent or an Affiliate) on page 226
- SEA Rule 15c3-1(c)(2)(iv)(B)/16 (Deficits or Unsecured Balances in Securities Transactions with a Federal Reserve Bank) on page 283
- SEA Rule 15c3-1(c)(2)(iv)(C)/095 (Unsecured Receivables and Related Payables) on page 298

- SEA Rule 15c3-1(c)(2)(viii)(C)/033 (Offsetting Sale Commitments in an Unregistered Offering) on page 653
- SEA Rule 15c3-1(e)/01 (Services Arrangement with a Parent or an Affiliate) on page 855
- SEA Rule 15c3-3(j)(2)(ii)(B)(3)(i)(C)/01 (Changing, Adding or Deleting Products Available Through a Sweep Program) on page 2467
- SEA Rule 15c3-3(Exhibit A - Note E(5))/02 (Exclusion of Omnibus Accounts from the Requirements of Note E(5)) on page 2606
- SEA Rule 15c3-3(Exhibit A - General)/012 (Netting a Customer's Account Balances when Preparing the Reserve Formula Computation under the Alternative Standard) on page 2622
- SEA Rule 15c3-3 (Exhibit A - Item 10)/10 (Term Debits in Customers' Accounts Collateralized by Securities Subject to Restrictions on Use) on page 2729

The following interpretations have been **revised**:

- SEA Rule 15c3-1(a)/01 (Additional Net Capital Requirement) on page 1
- SEA Rule 15c3-1(c)(1)/11 (Accrued Liability for Concessions or Commissions Payable) on page 153
- SEA Rule 15c3-1(c)(2)(iv)(C)/091 (Concessions Receivable from Individual Variable Annuities are Allowable for 30 Days; from Group Variable Annuities an Offset is Permitted) on page 296
- SEA Rule 15c3-1(c)(2)(viii)(C)/032 (Offsetting Sale Commitments in a Registered Offering) on page 653
- SEA Rule 15c3-3(a)(1)/01 (Customer/Non-Customer Classification) on page 2003
- SEA Rule 15c3-3 (Exhibit A - Item 10)/07 (Debit Balances in Customers' Accounts Collateralized by Control or Restricted Securities) on page 2728

The following interpretations have been **rescinded**:

- SEA Rule 15c3-1(c)(2)(iv)(C)/09 (Commissions or Concessions Receivable versus Commissions or Concessions Payable) on page 296
- SEA Rule 15c3-3(Exhibit A - Item 11)/041 (Federal Reserve Bank as a Non-Customer) on page 2744

The rule text update is available in portable digital format (pdf) on FINRA's Interpretations of Financial and Operational Rules page.

FINRA member firms and others that maintain the hardcopy version of the Interpretations of Financial and Operational Rules may refer to the accompanying updated page, containing the update, which is being made available to enable the replacement of existing pages in the hardcopy version of the Interpretations of Financial and Operational Rules. The filing instructions for the new page(s) are as follows:

SEA Rule	Remove Old Pages	Add New Pages
15c3-1	1	1
15c3-1	153	153
15c3-1	158	158
15c3-1	181-182	180-182
15c3-1	225	225-226
15c3-1	283	283
15c3-1	296-298	296-298
15c3-1	653-654	653-654
15c3-1	854	854-855
15c3-3	2003	2003
15c3-3	2467	2467
15c3-3	2606	2606
15c3-3	2622-2623	2622-2623
15c3-3	2727-2729	2727-2729
15c3-3	2744	2744

Further, the SEC staff continues to communicate and issue written and oral interpretations of the financial responsibility and reporting rules. FINRA will update the Interpretations of Financial and Operational Rules on its website as these written and oral interpretations are issued.

Regulatory Notice 21-29

Vendor Management and Outsourcing

FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors

Summary

Member firms are increasingly using third-party vendors to perform a wide range of core business and regulatory oversight functions. FINRA is publishing this *Notice* to remind member firms of their obligation to establish and maintain a supervisory system, including written supervisory procedures (WSPs), for any activities or functions performed by third-party vendors, including any sub-vendors (collectively, Vendors) that are reasonably designed to achieve compliance with applicable securities laws and regulations and with applicable FINRA rules. This *Notice* reiterates applicable regulatory obligations; summarizes recent trends in examination findings, observations and disciplinary actions; and provides questions member firms may consider when evaluating their systems, procedures and controls relating to Vendor management.

This *Notice*—including the "Questions for Consideration" below—does not create new legal or regulatory requirements or new interpretations of existing requirements. Many of the reports, tools or methods described herein reflect information firms have told FINRA they find useful in their Vendor management practices. FINRA recognizes that there is no one-size-fits-all approach to Vendor management and related compliance obligations, and that firms use risk-based approaches that may involve different levels of supervisory oversight, depending on the activity or function Vendors perform. Firms may consider the information in this *Notice* and employ the practices that are reasonably designed to achieve compliance with relevant regulatory obligations based on the firm's size and business model.

FINRA also notes that the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency recently published and requested comment on proposed guidance designed to help banking organizations manage risks associated with third-party relationships. FINRA will monitor this proposed guidance and consider comparable action, where appropriate.

August 13, 2021

Notice Type

- Guidance

Suggested Routing

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

Key Topics

- Business Continuity Planning (BCP)
- Cybersecurity
- Due Diligence
- Internal Controls
- Supervision
- Vendor Management

Referenced Rules & Notices

- FINRA Rule 1220
- FINRA Rule 3110
- FINRA Rule 4311
- FINRA Rule 4370
- Regulation S-P Rule 30
- Notice to Members 05-48

Questions or comments concerning this *Notice* may be directed to:

- Ursula Clay, Senior Vice President and Chief of Staff, Member Supervision, at 646-315-7375 or Ursula.Clay@finra.org;
- Sarah Kwak, Associate General Counsel, Office of General Counsel, at 202-728-8471 or Sarah.Kwak@finra.org;
- Michael MacPherson, Senior Advisor, Member Supervision, at 646-315-8449 or Michael.MacPherson@finra.org.

Background and Discussion

In 2005, FINRA published *Notice to Members 05-48* (Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers), which identified a number of common activities or functions that member firms frequently outsourced to Vendors, including "accounting/finance (payroll, expense account reporting, etc.), legal and compliance, information technology (IT), operations functions (*e.g.,* statement production, disaster recovery services, etc.) and administration functions (*e.g.,* human resources, internal audits, etc.)." Since that time, including during the COVID-19 pandemic, member firms have continued to expand the scope and depth of their use of technology and have increasingly leveraged Vendors to perform risk management functions and to assist in supervising sales and trading activity and customer communications.[1]

FINRA encourages firms that use—or are contemplating using—Vendors to review the following obligations and assess whether their supervisory procedures and controls for outsourced activities or functions are sufficient to maintain compliance with applicable rules.

CATEGORY	SUMMARY OF REGULATORY OBLIGATIONS
Supervision	FINRA Rule 3110 (Supervision) requires member firms to establish and maintain a system to supervise the activities of their associated persons that is reasonably designed to achieve compliance with federal securities laws and regulations, as well as FINRA rules, including maintaining written procedures to supervise the types of business in which it engages and the activities of its associated persons. This supervisory obligation extends to member firms' outsourcing of certain "covered activities"—activities or functions that, if performed directly by a member firm, would be required to be the subject of a supervisory system and WSPs pursuant to FINRA Rule 3110.[2] *Notice* 05-48 reminds member firms that "outsourcing an activity or function to ... [a Vendor] does not relieve members of their ultimate responsibility for compliance with all applicable federal securities laws and regulations and [FINRA] and MSRB rules regarding the outsourced activity or function." Further, *Notice* 05-48 states that if a member outsources certain activities, "the member's supervisory system and [WSPs] must include procedures regarding its outsourcing practices to ensure compliance with applicable securities laws and regulations and [FINRA] rules." FINRA expects member firms to develop reasonably designed supervisory systems appropriate to their business model and scale of operations that address technology governance-related risks, such as those inherent in firms' change and problem-management practices. Failure to do so can expose firms to operational failures that may compromise their ability to serve their customers or comply with a range of rules and regulations, including FINRA Rules 4370 (Business Continuity Plans and Emergency Contact Information), 3110 (Supervision) and books and records requirements under 4511 (General Requirements), as well as Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3 and 17a-4.

CATEGORY	SUMMARY OF REGULATORY OBLIGATIONS
Registration	*Notice* 05-48 reminds firms that, "in the absence of specific [FINRA] rules, MSRB rules, or federal securities laws or regulations that contemplate an arrangement between members and other registered broker-dealers with respect to such activities or functions (*e.g.,* clearing agreements executed pursuant to [FINRA Rule 4311]), any third-party service providers conducting activities or functions that require registration and qualification under [FINRA] rules will generally be considered associated persons of the member and be required to have all necessary registrations and qualifications." Accordingly, firms must review whether Vendors or their personnel meet any registration requirements under FINRA Rule 1220 (Registration Categories), as well as whether employees of the member firm are "Covered Persons" under the Operations Professional registration category pursuant to FINRA Rule 1220(b)(3), due to their supervision of "Covered Functions" executed by a Vendor or because they are authorized or have the discretion materially to commit the member firm's capital in direct furtherance of a Covered Function or to commit the member firm to any material contract or agreement (written or oral) with a Vendor in furtherance of a Covered Function.
Cybersecurity	SEC Regulation S-P Rule 30 requires broker-dealers to 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: (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. FINRA expects member firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations. FINRA reminds member firms to review core principles and effective practices for developing such programs and controls, including Vendor management, from our Report on Cybersecurity Practices (2015 Report) and the Report on Selected Cybersecurity Practices – 2018 (2018 Report), as well as other resources included in the Appendix to this *Notice*.

CATEGORY	SUMMARY OF REGULATORY OBLIGATIONS
Business Continuity Planning (BCP)	FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) requires member firms to create and maintain a written BCP with procedures that are reasonably designed to enable member firms to meet their existing obligations to customers, counterparties and other broker-dealers during an emergency or significant business disruption. The elements of each member firm's BCP—including their use of Vendors—can be "flexible and may be tailored to the size and needs of a member [firm]," provided that minimum enumerated elements are addressed. As a reminder, member firms must review and update their BCPs, if necessary, in light of changes to member firms' operations, structure, business or location.

Exam Findings and Observations

The 2021 Report on FINRA's Exam and Risk Monitoring Program, as well as our 2019, 2018 and 2017 Reports on FINRA Examination Findings, addressed compliance deficiencies (discussed below) arising from firms' Vendor relationships.

Cybersecurity and Technology Governance

- **Vendor Controls** – Firms failed to document or implement procedures to: 1) evaluate prospective and, as appropriate, test existing Vendors' cybersecurity controls, or 2) manage the lifecycle of their engagement with Vendors (*i.e.,* from onboarding, to ongoing monitoring, through off-boarding, including defining how Vendors dispose of customer non-public information).
- **Access Management** – Firms failed to implement effective Vendor access controls, including: limiting and tracking Vendors with administrator access to firm systems; instituting controls, such as a "policy of least privilege," to grant system and data access to Vendors only when required and removing access when no longer needed; or implementing multi-factor authentication for Vendors and contractors.
- **Inadequate Change Management Supervision** – Firms did not perform sufficient supervisory oversight of Vendors' application and technology changes impacting firm business and compliance processes, especially critical systems (including upgrades, modifications to or integration of member firm or Vendor systems). These oversight failures led to violations of regulatory obligations, such as those relating to data integrity, cybersecurity, books and records and confirmations.
- **Limited Testing of System Changes and Capacity** – Firms did not adequately test changes to, or system capacity of, order management, account access and trading algorithm systems, and thus failed to detect underlying malfunctions or capacity constraints.
- **Data Loss Prevention Programs** – Vendors did not encrypt confidential firm and customer data (*e.g.,* Social Security numbers) stored at Vendors or in transit between firms and Vendors.

FINRA Disciplined Firms Whose Vendors Did Not Implement Technical Controls

FINRA disciplined certain firms for violations of Regulation S-P Rule 30 and FINRA Rules 3110 and 2010 for failing to maintain adequate procedures and execute supervisory oversight to protect the confidentiality of their customers' nonpublic personal information, including, for example, where:

- a Vendor exposed to the public internet the firms' purchase and sales blotters, which included customers' nonpublic personal information (*e.g.,* names, account numbers, and social security numbers).
- a Vendor did not configure its cloud-based server correctly, install antivirus software, and implement encryption for the firm's account applications and other brokerage records containing customers' nonpublic personal information. As a result, foreign hackers successfully accessed the cloud-based server and exposed firm customers' nonpublic personal information.

Books and Records

- Firms failed to perform adequate due diligence to verify Vendors' ability to maintain books and records on behalf of member firms in compliance with Exchange Act Rules 17a-3 and 17a-4, as well as FINRA Rule 3110(b)(4) (Review of Correspondence and Internal Communications) and FINRA Rule Series 4510 (Books and Records Requirements) (collectively, Books and Records Rules).
- Firms failed to confirm that service contracts and agreements comply with requirements to provide notification to FINRA under Exchange Act Rule 17a-4(f)(2)(i), including a representation that the selected electronic storage media (ESM) used to maintain firms' books and records meets the conditions of Exchange Act Rule 17a-4(f)(2) and a third-party attestation as set forth in Exchange Act Rule 17a-4(f)(3)(vii) (collectively, ESM Notification Requirements).
- Firms did not confirm that Vendors complied with contractual and regulatory requirements to maintain (and not delete, unless otherwise permitted) firms' books and records.[3]

Consolidated Account Reports (CARs) – Firms did not have processes in place to evaluate how they and registered representatives selected CARs Vendors; set standards for whether and when registered representatives were authorized to use Vendor-provided CARs; determine when and how registered representatives could add manual entries or make changes to CARs; test or otherwise validate data for non-held assets reported in CARs (or clearly and prominently disclose that the information provided for those assets was unverified); and maintain records of CARs.[4]

Fixed Income Mark-up Disclosure – Firms failed to test whether Vendors identified the correct prevailing market price (PMP) from which to calculate mark-ups and mark-downs (for example, instead of using the prices of a member firm's own contemporaneous trades, which were available to be considered, a Vendor's program incorrectly identified PMPs using lower levels of the "waterfall" as described in FINRA Rule 2121.02 (Additional Mark-Up Policy For Transactions in Debt Securities, Except Municipal Securities) or MSRB Rule G-30.06 (Mark-Up Policy).

FINRA Disciplined Firms for Books and Records Violations Resulting from Vendor Deficiencies

FINRA disciplined firms for violations of Books and Records rules and related supervisory obligations involving Vendors, including, but not limited to, failing to preserve and produce business-related electronic communications (including emails, social media, texts, instant messages, app-based messages and video content) due to:

- Vendors' system malfunctions;
- Vendors' data purges after termination of their relationship with firms;
- Vendors failing to correctly configure default retention periods resulting in inadvertent deletions of firm electronic communication for certain time periods;
- Vendors' system configurations making deleted emails unrecoverable after 30 days;
- Vendors failing to provide non-rewriteable, non-erasable storage; and
- Firms failing to establish an audit system to account for Vendors' preservation of emails.

Questions for Consideration

The following questions may help firms evaluate whether their supervisory control system, including WSPs, adequately addresses issues and risks relating to Vendor management. The questions—which address both regulatory requirements and effective practices FINRA has observed firms implement—focus on four phases of a firm's outsourcing activities:

- deciding to outsource an activity or function,
- conducting due diligence on prospective Vendors,
- onboarding Vendors, and
- overseeing or supervising outsourced activities or functions.

As noted above, firms should not infer any new obligations from the questions for consideration. Many of the reports, tools or methods described herein reflect information firms have told FINRA they find useful in their vendor management practices. FINRA is sharing this information for firms' consideration only.

Firms may wish to evaluate the questions presented below in the context of a risk-based approach to Vendor management in which the breadth and depth of their due diligence and oversight may vary based on the activity or function outsourced to a Vendor. Factors firms may take into consideration include, but are not limited to:

- Will the Vendor be handling sensitive firm or customer non-public information?
- What would be the extent of the potential damage if there is a security breach (*e.g.,* number of customers or prospective customers impacted)?
- Is the Vendor performing a business-critical role or fulfilling a regulatory requirement for the firm?
- What is the reputation and history of the Vendor, including the representations made and information shared on how the Vendor will secure the firm's information?

I. Decision to Outsource

A decision to outsource an activity or function may depend, in part, on whether the firm has an adequate process to make that determination and then to supervise that outsourced activity or function. The following considerations may help firms address those threshold questions.

- Does your firm have a process for its decision-making on outsourcing, including the selection of Vendors?
- Does your firm's supervisory control system address your firm's outsourcing practices, including your firm's approach to Vendor due diligence?
- Does your firm identify risks that may arise from outsourcing a particular activity or function and consider the impact of such outsourcing on its ability to comply with federal securities laws and regulations, and FINRA rules?
- Does your firm engage key internal stakeholders (*e.g.,* Compliance, Legal, IT or Risk Management) relevant to, and with the requisite experience to assess, the outsourcing decision?

II. Due Diligence

Once a member firm decides to outsource an activity or function, it may want to consider some or all of the following questions in evaluating and selecting potential Vendors:

- Due Diligence Approach
  - What factors does your firm consider when conducting due diligence on potential Vendors? These may include, but are not limited to: a Vendors' financial condition, experience and reputation; familiarity with regulatory requirements, fee structure and incentives; the background of Vendors' principals, risk management programs, information security controls, and resilience.

- If a potential Vendor will be performing a function that is subject to regulatory requirements, how does your firm evaluate whether the Vendor has the ability to comply with applicable regulatory requirements and undertakings (*e.g.,* Book and Records rules, including ESM Notification Requirements)?
- Does your firm consider obtaining evaluations of prospective Vendors' SSAE 18, Type II, SOC 2 (System and Organization Control) reports (if available)? If so, who reviews the evaluations and how does your firm follow up on any identified concerns, including, for example, those related to cybersecurity?
- Does your firm take a risk-based approach to vendor due diligence? Does the scope and depth of your firm's due diligence reflect the degree of risk associated with the activities or functions that will be outsourced?
- Does your firm evaluate the impact to your customers or firm if a Vendor fails to perform, for example, by not fulfilling a regulatory obligation? What measures can your firm put in place to mitigate that risk?
- Does your firm assess the BCPs of prospective Vendors that would perform critical business, operational, risk management or regulatory activities or functions?
- If a Vendor will likely be conducting activities or functions that require registration under FINRA rules, does your firm have a process for determining whether the Vendor's personnel will be appropriately qualified and registered?
- Does your firm evaluate Vendors' controls and due diligence of Vendors' sub-contractors, particularly if the sub-contractor may have access to sensitive firm or customer non-public information or critical firm systems?
- Does your firm include individuals with the requisite expertise and experience in the due diligence process—including with respect to cybersecurity, information technology, risk management, business functions and relevant regulatory obligations—to effectively evaluate potential Vendors? How does your firm handle instances where your firm does not have the expertise or experience in-house?
- Does your firm document its due diligence findings?

- **Conflicts of Interest –** Does your firm put controls in place to mitigate potential conflicts of interest in the Vendor selection process? For example:
  - Does your firm require staff involved in its Vendor selection processes to disclose any personal relationship with the Vendor? If so, what steps does your firm take to assess whether that relationship may influence the choice of Vendor?
  - Does your firm allow staff to receive compensation or gifts from potential or current Vendors, which could influence the decision to select, or maintain a relationship with, a particular Vendor?

- **Cybersecurity**

Does your firm assess the Vendors' ability to protect sensitive firm and customer non-public information and data? Does your firm have access to expertise to conduct that assessment? (See also question, above, regarding SSAE 18 Type II, SOC 2 reports.)

III. Vendor Onboarding

After completing due diligence and selecting a Vendor, firms may wish to consider putting in place a written contract with the Vendor that addresses, among other things, both the firm's and the Vendor's roles with respect to outsourced regulatory obligations.

- **Vendor Contracts**
  - Does your firm document relationships with Vendors in a written contract, and if not, under what circumstances?
  - Do your firm's contracts address, when applicable, Vendors' obligations with respect to such issues as:
    - documentation evidencing responsible parties' and Vendors' compliance with federal and state securities laws and regulations and FINRA rules (*e.g.,* retention period required for preservation of firm records);
    - non-disclosure and confidentiality of information;
    - protection of non-public, confidential and sensitive firm and customer information;
    - ownership and disposition of firm and customer data at the end of the Vendor relationship;
    - notification to your firm of cybersecurity events and the Vendor's efforts to remediate those events, as well as notification of data integrity and service failure issues;
    - Vendor BCP practices and participation in your firm's BCP testing, including frequency and availability of test results;
    - disclosure of relevant pending or ongoing litigation;
    - relationships between Vendors, sub-contractors and other third-parties;
    - firm and regulator access to books and records; and
    - timely notification to your firm of application or system changes that will materially affect your firm.
  - Do your firm's contracts with Vendors address roles, responsibilities and performance expectations with respect to outsourced activities or functions?

- **Features and Default Settings of Vendor Tools**
  - Does your firm review, and as appropriate adjust, Vendor tool default features and settings, such as to limit use of communication tools to specific firm-approved features (*e.g.,* disabling a chat feature, or reviewing whether the communications are being captured for supervisory review), to set the appropriate retention period for data stored on a vendor platform or to limit data access—to meet your firm's business needs and applicable regulatory obligations?

IV. Supervision

Member firms have a continuing responsibility to oversee, supervise and monitor the Vendor's performance of the outsourced activity or function. Firms may wish to consider the following potential steps in determining how they fulfill this supervisory obligation:

- Obtaining representations from the Vendor in a contractual agreement that they are conducting self-assessments and undertaking the specific responsibilities identified;
- Requiring Vendors to provide attestations or certifications that they have fulfilled certain reviews or obligations;
- Going onsite to Vendors to conduct testing or observation, depending on the firm's familiarity with the vendor or other risk-based factors;
- Monitoring and assessing the accuracy and quality of the Vendor's work product;
- Remaining aware of news of Vendor deficiencies and investigating whether they are indicative of a problem with an activity or function the Vendor is performing for your firm;
- Investigating customer complaints that may be indicative of issues with a Vendor and exploring whether there are further-reaching impacts; and
- Training staff to address and escalate red flags at your firm that a Vendor may not be performing an activity or function adequately, such as not receiving confirmation that a Vendor task was completed.

In addition to the above, firms may want to consider asking the following questions, where applicable, with respect to more specific aspects of their supervisory system.

- **Supervisory Control System**
  - Does your firm monitor Vendors (for example, by reviewing SOC 2 reports) and document results of its ongoing supervision, especially for critical business or regulatory activities or functions?
  - Do your firm's WSPs address roles and responsibilities for firm staff who supervise Vendor activities?
  - Does your firm periodically review and update its Vendor management-related WSPs to reflect material changes in the firm's business or business practices?

- **Business Continuity Planning**
  - Does your firm's business continuity planning and testing include Vendors? If so, what are the testing requirements for Vendors and how often are such tests performed? How do these tests inform your firm's overall BCP?
  - Does your firm have contingency plans for interruptions or terminations of Vendor services?
  - If there is a disaster recovery event, has your firm assessed whether the Vendor will have sufficient staff dedicated to your firm?
- **Cybersecurity and Technology Change Controls**
  - **Access Controls**
    - Does your firm know which Vendors have access to: (1) sensitive firm or customer non-public information and (2) critical firm systems?
    - Does your firm implement access controls through the lifecycle of its engagement with Vendors, including developing a "policy of least privilege" to grant Vendors system and data access only when required and revoke it when no longer needed and upon termination?
    - Has your firm considered implementing multi-factor authentication for Vendors and, if warranted, their sub-contractors?
  - **Cybersecurity Events and Data Breaches**
    - Does your firm conduct independent, risk-based reviews to determine if Vendors have experienced any cybersecurity events, data breaches or other security incidents? If so, does your firm evaluate the Vendors' response to such events?
    - If a cybersecurity breach occurred at your firm's Vendor, was your firm notified and, if so, how quickly? Did your firm follow its incident response plan for addressing such breaches?
  - **Technology Change Management**
    - If applicable, how does your firm become aware of, evaluate and, as appropriate, test the impact of changes Vendors make to their applications and systems, especially for critical applications and systems?

FINRA Disciplined Firms for Failure to Supervise Vendors

FINRA disciplined certain firms that violated FINRA Rules 2010 and 3110, among other rules, when they failed to establish and maintain supervisory procedures for their Vendor arrangements reasonably designed to:

- Review, verify or correct vendor-provided expense ratio and historical performance information for numerous investment options in defined contribution plans (*i.e.,* retirement plans), causing firms' customer communications to violate FINRA Rule 2210;
- Oversee, monitor and evaluate changes and upgrades to automated rebalancing and fee allocation functions outsourced to a Vendor for wealth management accounts custodied at the firm, causing errors and imposing additional fees to customer accounts;
- Review, test or verify the accuracy and completeness of data feeds from Vendors that failed to identify the firm's prior role in transactions for issuers covered by firm research reports, resulting in violations of then NASD Rule 2711(h) and 2241(c) when the firm failed to make required disclosures in its equity research reports regarding its status as a manager or a co-manager of a public offering of the issuer's equity securities; and
- Confirm the accuracy and completeness of information provided by Vendors to regulators, including FINRA, both in response to specific requests and as part of regular trade and other reporting obligations, causing inaccurate responses and misreported transactions, order reports, route reports and reportable order events.

Conclusion

As noted throughout this *Notice*, the requirement that a member firm maintain a reasonably designed supervisory system and associated WSPs extends to activities or functions it may outsource to a Vendor. While the manner and frequency by which these activities or functions are overseen is determined by the member firm, and is dependent on a number of factors, the information in this *Notice* is intended to provide firms with ideas and questions they can use to build and evaluate the sufficiency of their Vendor management protocols. Additional helpful resources can be found in the Appendix.

Endnotes

1. *See Regulatory Notice* 20-42 (FINRA Seeks Comment on Lessons from the COVID-19 Pandemic); COVID-19/Coronavirus Topic Page; *Regulatory Notice* 20-16 (FINRA Shares Practices Implemented by Firms to Transition to, and Supervise in, a Remote Work Environment During the COVID-19 Pandemic); and *Regulatory Notice* 20-08 (Pandemic-Related Business Continuity Planning, Guidance and Relief).

2. *See also* NASD Office of General Counsel, Regulatory Policy and Oversight Interpretive Guidance, which clarified that *Notice 05-48* was issued to provide guidance on a member's responsibilities if the member outsources certain activities and was not intended to address the appropriateness of outsourcing a particular activity or whether an activity could be outsourced to a non-broker-dealer third-party service provider.

3. *See Regulatory Notice* 18-31 (SEC Staff Issues Guidance on Third-Party Recordkeeping Services).

4. *See Regulatory Notice* 10-19 (FINRA Reminds Firms of Responsibilities When Providing Customers with Consolidated Financial Account Reports).

Appendix – Additional Resources

Regulatory Notices and Guidance

- **Outsourcing and Vendor Management**
  - *Regulatory Notice* 11-14 (FINRA Requests Comment on Proposed New FINRA Rule 3190 to Clarify the Scope of a Firm's Obligations and Supervisory Responsibilities for Functions or Activities Outsourced to a Third-Party Service Provider)
  - *Notice to Members* 05-48 (Members' Responsibilities When Outsourcing Activities to Third-Party Providers), and NASD Office of General Counsel, Regulatory Policy and Oversight Interpretive Guidance
  - *Regulatory Notice* 18-31 (SEC Staff Issues Guidance on Third-Party Recordkeeping Services)
- **Cybersecurity**
  - Report on Selected Cybersecurity Practices – 2018
  - Report on Cybersecurity Practices – 2015

FINRA Examination Findings Reports

- 2021 Report on FINRA's Examination and Risk Monitoring Program
- 2019 Report on FINRA Examination Findings and Observations
- 2018 Report on FINRA Examination Findings
- 2017 Report on FINRA Examination Findings

Tools

- Core Cybersecurity Controls for Small Firms
- Small Firm Cybersecurity Checklist
- Outsourcing and Vendor Management section of the Peer-2-Peer Compliance Library
  - Outsourcing Due Diligence Form
  - Sample Vendor On-Site Audit Template
  - Sample Vendor Questionnaire
  - Third Party Matrix
  - Third Party Vendor Contracts Sample Language
  - Vendor Management Considerations
  - Vendor Security Questionnaire

2022 Annual Conference

May 16 –18 | Washington, DC | Hybrid Event

Hot Topics in Municipal Securities and Other Fixed Income

Tuesday, May 17, 2022
11:00 a.m. – 12:00 p.m.

FINRA and MSRB staff discuss recent enforcement actions related to municipal securities (e.g., 529 Plans, municipal short positions), examination priorities, fixed income-related rulemaking and common problems uncovered during Member Supervision and Market Regulation reviews.

Moderator:

Cynthia Friedlander
Senior Director, Fixed Income Regulation
FINRA Office of General Counsel

Panelists:

Gene Davis
Director, Fixed Income Program
FINRA Member Supervision

Bri Joiner
Director, Regulatory Compliance
Municipal Securities Rulemaking Board (MSRB)

John Saxton
Senior Director, Trading and Execution (T&E) Fixed Income Examination
FINRA Market Regulation

Hot Topics in Municipal Securities and Other Fixed Income Panelists Bios:

Moderator:

Cynthia Friedlander is Senior Director of Fixed Income Regulation in FINRA's Office of General Counsel. Ms. Friedlander is responsible for directing the design, development and delivery of fixed income-related examination and policy guidance to FINRA staff, as well as to member firms, and is FINRA's primary liaison to the Municipal Securities Rulemaking Board and the Securities and Exchange Commission's Office of Municipal Securities. Ms. Friedlander represents FINRA at government agency, SRO, industry and advisory meetings and is a staff liaison to FINRA's Fixed Income Committee. She holds a B.A. in government from the University of Virginia and an M.B.A. with a concentration in finance from George Mason University.

Panelists:

Gene C. Davis is Director of FINRA's Fixed Income Specialist Team. The Fixed Income Specialist Team is responsible for conducting higher risk fixed income examinations and those of firms engaged in a material fixed income business. Mr. Davis has been with FINRA (formerly NASD) since February 1997 and has participated in numerous matters of member firms engaged in a myriad of fixed income business lines. Mr. Davis has completed the FINRA Institute at Wharton Certificate Program, obtaining the Certified Regulatory and Compliance Professional™ (CRCP™) designation in 2004.

Bri Joiner is Director of Regulatory Compliance at the Municipal Securities Rulemaking Board (MSRB), in which she oversees a portfolio of programs under the MSRB's Market Regulation department, maintaining responsibility for strategic planning and execution of long-term objectives. Ms. Joiner is directly responsible for the MSRB's professional qualifications program, examiner training program and regulatory compliance program initiatives. Prior to assuming her current role, Ms. Joiner managed the MSRB's regulatory education program leading the development and delivery of content for regulated entities and market stakeholders in support of a fair and efficient municipal securities market. Prior to joining the MSRB, Ms. Joiner spent 10 years at the Financial Industry Regulatory Authority (FINRA). She served as Senior Regulatory Policy Analyst in FINRA's Office of General Counsel, where she worked on rulemaking initiatives and researched legal and compliance matters. She also held the position of Senior Manager in FINRA's Member Education and Training department, where she advised on initiatives having a market impact and served as a subject matter expert on various topics. Ms. Joiner began her career at the U.S. Securities and Exchange Commission. Ms. Joiner earned a bachelor's degree, *magna cum laude*, from Spelman College and a juris doctor from the Walter F. George School of Law, Mercer University. She is a member of Phi Beta Kappa Honor Society, Golden Key International Honour Society and Phi Delta Phi Legal Fraternity.

John Saxton is Senior Director in FINRA's Division of Market Regulation. He joined FINRA/New York Stock Exchange in 1997 and currently leads the Trading and Execution Fixed Income Examination team. This specialized team is responsible for conducting trading and execution reviews in fixed income securities within FIRNA's cycle examination program. Prior to his current role, Mr. Saxton was a Senior Director in FINRA's Division of Market Regulation supervising several surveillance teams and was a Trial Counsel in NYSE's Division of Enforcement. Mr. Saxton earned his J.D. from New York Law School and a B.S. in Business Administration from St. Michael's College.

Hot Topics in Municipal Securities and Other Fixed Income

Panelists

- **Moderator**
  - Cynthia Friedlander, Senior Director, Fixed Income Regulation, FINRA Office of General Counsel
- **Panelists**
  - Gene Davis, Director, Fixed Income Program, FINRA Member Supervision
  - Bri Joiner, Director, Regulatory Compliance, Municipal Securities Rulemaking Board (MSRB)
  - John Saxton, Senior Director, Examinations Trading and Execution (T&E) Fixed Income Examination, FINRA Market Regulation

Hot Topics in Municipal Securities and Other Fixed Income
Tuesday, May 17, 2022
11:00 a.m. – 12:00 p.m.

Resources:

FINRA Resources:

- 2022 Report on FINRA's Examination and Risk Monitoring Program

  www.finra.org/sites/default/files/2022-02/2022-report-finras-examination-risk-monitoring-program.pdf

- Firm Short Positions and Fails-to-Receive in Municipal Securities

  www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program/firm-short-positions-fails-receive

- Communications with the Public: Regulatory Obligations and Related Considerations

  www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program/communication-with-public

- Best Execution: Regulatory Obligations and Related Considerations

  www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program/best-execution

- Fixed Income Confirmation Disclosure: Frequently Asked Questions (FAQ)

  www.finra.org/rules-guidance/key-topics/fixed-income/confirmation-disclosure-faq

- FINRA *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* (March 2021)

  www.finra.org/rules-guidance/notices/21-12

- FINRA *Regulatory Notice 16-30, FINRA Reminds Firms of their Obligation to Report Accurately the Time of Execution for Transactions in TRACE-eligible Securities* (August 2016)

  www.finra.org/rules-guidance/notices/16-30

- FINRA *Regulatory Notice 15-27, Guidance Relating to Firm Short Positions and Fails-to-Receive in Municipal Securities* (July 2015)

  www.finra.org/rules-guidance/notices/15-27

Other Resources:

- SEC *No-action Letter Regarding Rule 15c2-11 and Fixed Income Securities*

www.sec.gov/files/fixed-income-rule-15c2-11-nal-finra-121621.pdf

- Market Discount on Municipal Securities Transactions
    - MSRB *Interpretive Notice Regarding Rule G-47, on Time of Trade Disclosure – Disclosure of Market Discount* (November 22, 2016)

      www.msrb.org/Rules-and-Interpretations/MSRB-Rules/General/Rule-G-47?tab=2
    - MSRB *Issue Brief: Tax and Liquidity Considerations for Buying Discount Bonds*

      www.msrb.org/-/media/Files/Resources/Tax-and-Liquidity-Considerations-for-Buying-Discount-Bonds.ashx?

- MSRB *Interpretive Notice 2021-12, Request for Input on Draft Compliance Resources for Dealers and Municipal Advisors Concerning New Issue Pricing* (October 2021)

  www.msrb.org/-/media/Files/Regulatory-Notices/RFCs/2021-12.ashx??n=1

- Implementation Guidance on MSRB Rule G-18, on Best Execution (November 2015)

  www.msrb.org/Rules-and-Interpretations/MSRB-Rules/General/Rule-G-18?tab=2#_4A7607BC-365C-47BE-9E17-69F0E3A0F036

Enforcement Actions:

- Municipal Short Positions
    - *Merrill Lynch, Pierce, Fenner & Smith Incorporated*, Matter #2016050801701 (FINRA AWC October 2021)

      www.finra.org/sites/default/files/fda_documents/2016050801701%20Merrill%20Lynch%2C%20Pierce%2C%20Fenner%20%26%20Smith%20Incorporated%20CRD%207691%20AWC%20sl%20%282021-1635985222715%29.pdf
    - *UBS Financial Services Inc.*, Matter #2016050874301 (FINRA AWC October 2019)

      www.finra.org/sites/default/files/fda_documents/2016050874301%20UBS%20Financial%20Services%20Inc.%20CRD%208174%20AWC%20jm%20%282019-1572653998708%29.pdf

- Supervision of 529 Plan Share Class Recommendations
    - *UBS Financial Services Inc.*. Matter #2019062532801 (FINRA AWC December 2021)

      www.finra.org/sites/default/files/fda_documents/2019062532801%20UBS%20Financial%20Services%20Inc.%20CRD%208174%20AWC%20jlg%20%282022-1642724432927%29.pdf
    - *MML Investors Services, LLC*, Matter #2019062530501 (FINRA AWC December 2021)

      www.finra.org/sites/default/files/fda_documents/2019062530501%20MML%20Investors%20Services%2C%20LLC%20CRD%2010409%20AWC%20jlg%20%282022-1642724434897%29.pdf

- *Wells Fargo Advisors, LLC and Wells Fargo Advisors Financial Network, LLC*, Matter #2016049188701 (FINRA AWC December 2021)

  www.finra.org/sites/default/files/fda_documents/2016049188701%20Wells%20Fargo%20Advisors%2C%20LLC%20nka%20Wells%20Fargo%20Clearing%20Services%2C%20LLC%20CRD%2019616%20et%20al%20AWC%20sl%20%282022-1642638025722%29.pdf

- *Royal Alliance Associates, Inc.; Sagepoint Financial, Inc.; and FSC Securities Corporation*, Matter #2019062531501, (FINRA AWC October 2021)

  www.finra.org/sites/default/files/fda_documents/2019062531501%20Royal%20Alliance%20Associates%2C%20Inc.%20CRD%2023131%20et%20al%20AWC%20sl%20%282022-1642638026606%29.pdf

- *LPL Financial LLC*, Matter #2019062530101 (FINRA AWC October 2021)

  www.finra.org/sites/default/files/fda_documents/2019062530101%20LPL%20Financial%20LLC%20CRD%206413%20AWC%20sl%20%282022-1642638025474%29.pdf

Navigating Special Purpose Acquisition Companies (SPACs)
Tuesday, May 17, 2022
1:45 p.m. – 2:45 p.m.

The SPACs market has undergone rapid growth in recent years. Join FINRA staff as they discuss the difference between a SPAC and an IPO, and some of the risks of investing in SPACs.

Moderator:
Gabriela Aguero
Director, Public Offerings
FINRA Corporate Financing

Panelists:
Douglas Ellenoff
Partner
Ellenoff Grossman & Schole LLP

Osamu Watanabe
General Counsel
Moelis & Company

Jacob Yunger
Director, Financial Innovation
FINRA Office of Financial Innovation (OFI)

Navigating Special Purpose Acquisition Companies (SPACs) Panelists Bios:

Moderator:

Gabriela Aguero is Director in FINRA's Corporate Financing Department. In her role, she oversees the Public Offering Review (POR) program. The POR group is responsible for the review of a wide array of filings and the interpretation and application of FINRA's rules that regulate underwriting activities and conflicts of interests in public offerings. Ms. Aguero began her career at FINRA when she joined NASD in 2000. She has an MBA from the John's Hopkins Carey Business School in addition to an undergraduate degree in Finance as well as designation as a FINRA Certified Regulatory and Compliance Professional™ (CRCP™) Program at Wharton.

Panelists:

Douglas S. Ellenoff, a member of Ellenoff Grossman & Schole LLP founded in 1992, is a corporate and securities attorney with a focus in business transactions, mergers and acquisitions and corporate financings. Mr. Ellenoff has represented public companies in connection with their initial public offerings, secondary public offerings, regulatory compliance, as well as strategic initiatives and general corporate governance matters. During his career, he has represented numerous broker-dealers, venture capital investor groups and many corporations involved in the capital formation process. In the last several years, he has been involved at various stages in numerous registered public offerings, including more than 100 financings and, with other members of his firm, hundreds of private placements into public companies (see PIPEs and Venture Capital), representing either the issuers of those securities or the registered broker-dealers acting as placement agent. Along with other members of his Firm, Mr. Ellenoff has been involved at various stages with over 370 registered blind pool offerings (commonly referred to as "SPACs"); In addition to our IPO experience with SPACs, he has been involved with more than 80 SPAC M&A assignments. The Firm represents nearly 70 public companies with respect to their ongoing 34 Act reporting responsibilities and general corporate matters. He also provides counsel with regard to their respective ongoing (SEC, AMEX and NASD) regulatory compliance. Mr. Ellenoff and the rest of the corporate department distinguish themselves from many other transactional lawyers on the basis of their ability to be part of the establishment of new securities programs, like PIPEs, SPACs, Registered Directs and Reverse Mergers, where the Firm's professionals have played leadership roles within each of those industries, assisting in the creation, formation and strategies relating to those financings, as well as working closely with the regulatory agencies; including the SEC and FINRA; and the listing exchanges – AMEX and NASDAQ. Mr. Ellenoff is routinely requested to be a panelist and presenter at industry conferences.

Osamu Watanabe is the General Counsel of Moelis & Company, a leading independent investment bank listed on the NYSE. Mr. Watanabe joined Moelis & Company as a newly founded investment bank and managed its successful IPO. Mr. Watanabe was also General Counsel for Moelis Asset Management which includes MCP private equity funds, Gracie credit hedge funds, Freeport direct lending funds and Steele Creek CLO funds. Prior to joining Moelis & Company, Mr. Watanabe held senior positions at Sagent Advisors, UBS, Credit Suisse First Boston and Donaldson, Lufkin & Jenrette. Mr. Watanabe was in private practice at Sullivan & Cromwell in New York, Tokyo, Hong Kong and Melbourne for 10 years focusing on U.S. and international securities offerings, M&A transactions, restructurings, bank financings, real estate transactions, and broker-dealer, bank and investment company regulation. Mr. Watanabe clerked for the Honorable Morey L. Sear, Eastern District of Louisiana. Mr. Watanabe holds a B.A. from Antioch College (1982) and a J.D. from Yale Law School (1985).

Jacob Yunger is Director in the Office of Financial Innovation, studying a variety of topics including digital assets, decentralized finance, gamification, and SPACs. Prior to joining FINRA, Mr. Yunger had a career in portfolio and risk management for retail and institutional clients, spanning all asset classes but with a focus on the private markets. He earned a graduate degree in physics from Cornell University and an undergraduate degree in physics and philosophy from Yeshiva University.

Navigating Special Purpose Acquisition Companies (SPACs)

Panelists

- **Moderator**
  - Gabriela Aguero, Director, Public Offerings, FINRA Corporate Financing
- **Panelists**
  - Douglas Ellenoff, Partner, Ellenoff Grossman & Schole LLP
  - Osamu Watanabe, General Counsel, Moelis & Company
  - Jacob Yunger, Director, Financial Innovation, FINRA Office of Financial Innovation (OFI)

Agenda

01 | SPAC Basics

02 | SPAC Market – Supply & Demand

03 | The Future of SPACs

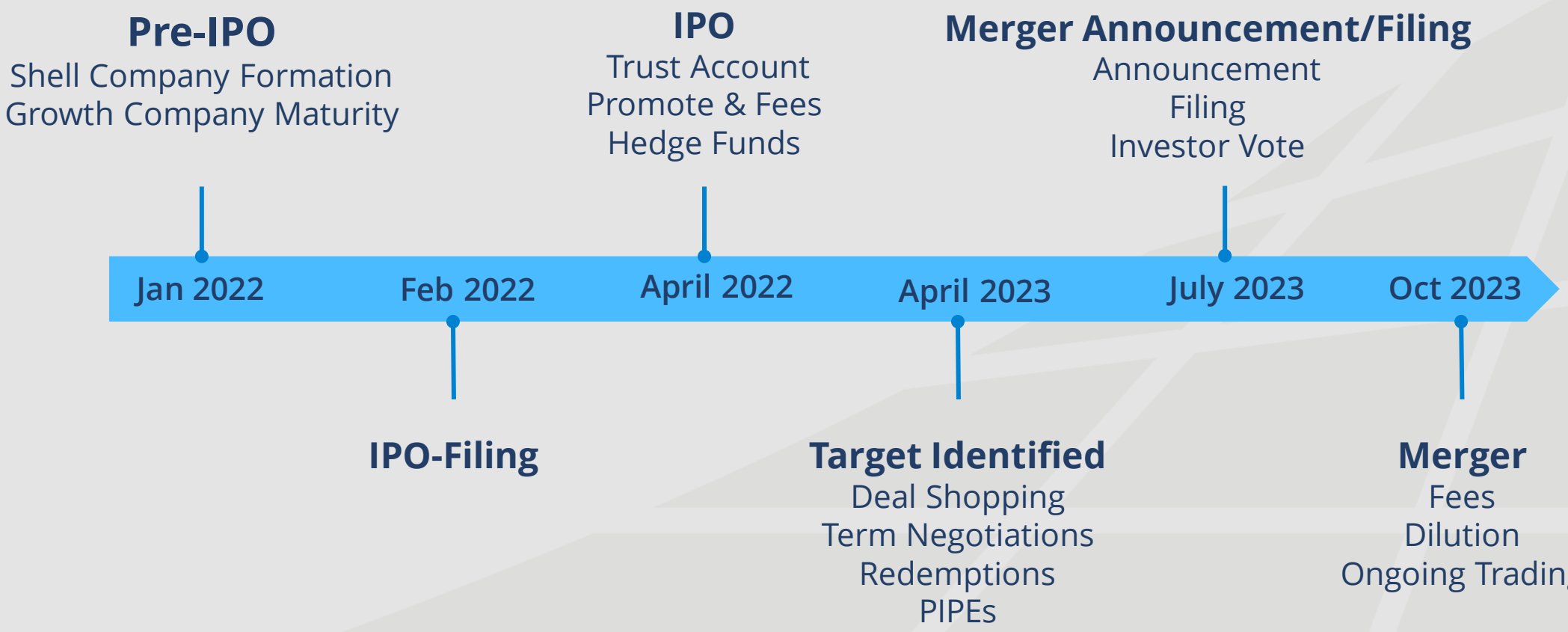
04 | Closing, Q & A

1 SPAC Basics

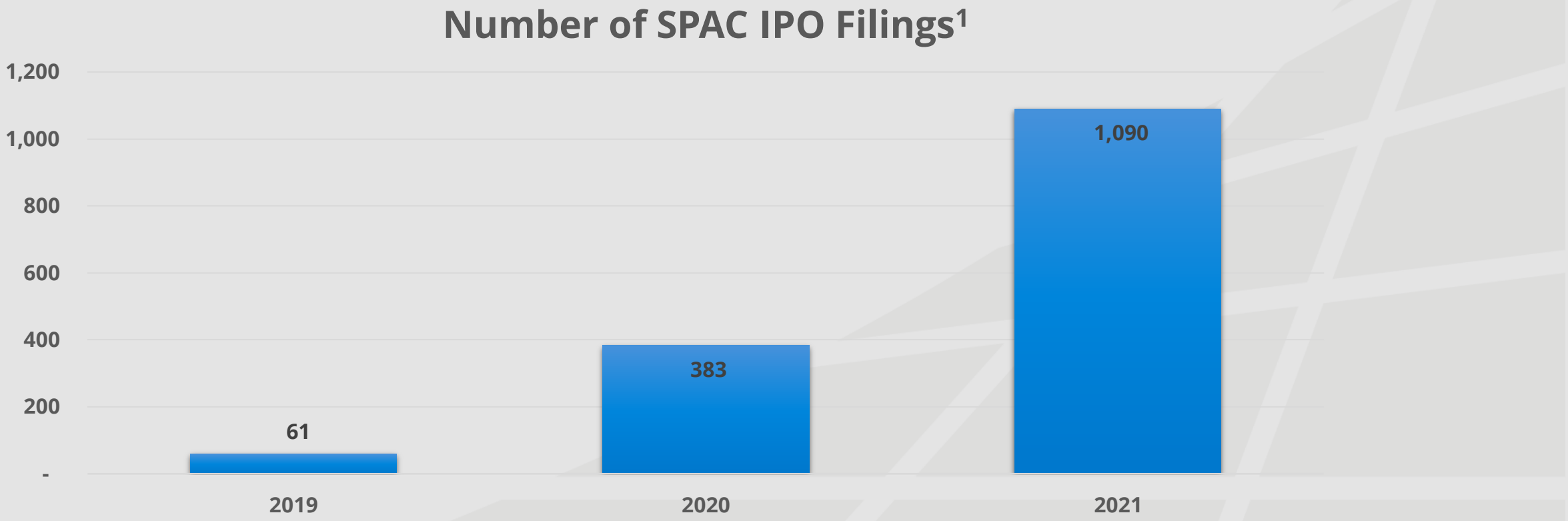
What are SPACs?

Shell companies that are created for one purpose: to raise capital in the public markets in order to merge with a privately held company.

Timeline of a SPAC



How many SPACs are there?



[1] https://www.finra.org/sites/default/files/2022-03/2022-industry-snapshot.pdf

2 | Developments in the SPAC Market

Demand & Supply

- Supply: Entrepreneur-Driven Solution
- Benefits: Capital, Innovation
- Demand: Private Equity / Hedge Funds / Portfolio Diversification

3 | Future of SPACs

SPACs Forward

- 600+ Sponsors looking for targets
- Market Reactions Disclosures/Projections/Financials
- Impact on capital formation and investor access
- Legal environment - underwriters

Reference Materials & Resources

- **SEC Proposal - Fact Sheet**
  - https://www.sec.gov/files/33-11048-fact-sheet.pdf

- **SEC's Proposed Rules**
  - https://www.sec.gov/rules/proposed/2022/33-11048.pdf

Navigating Special Purpose Acquisition Companies (SPACs)
Tuesday, May 17, 2022
1:45 p.m. – 2:45 p.m.

Resources:

- SEC Fact Sheet: SPACs, Shell Companies, and Projections

  www.sec.gov/files/33-11048-fact-sheet.pdf

- SEC Special Purpose Acquisition Companies, Shell Companies, and Projections Proposed Rules

  www.sec.gov/rules/proposed/2022/33-11048.pdf

2022 Annual Conference

May 16 –18 | Washington, DC | Hybrid Event

Changing Firms Digital Experience
Tuesday, May 17, 2022
1:45 p.m. – 2:45 p.m.

FINRA has created a culture of innovation and is an industry leader in the use of its technology tools and resources. Join FINRA panelists as they discuss FINRA's mission to change the digital experience for our member firms. During the session, learn about innovative ways FINRA is partnering with the industry to provide the best possible service.

Moderator:

Tigran Khrimian
Senior Vice President, Enterprise Data Platforms & Business Applications
FINRA Technology

Panelists:

Noah Egorin
Senior Director, Business Development & Innovation
FINRA Credentialing, Registration, Education and Disclosure (CRED)

Julia McCafferty
Director, Product Management
FINRA Technology

Michele Oswald
Team Leader
Edward Jones

Jennifer Szaro, CRCP®
Chief Compliance Officer
XML Securities, LLC

Changing Firms Digital Experience Panelists Bios:

Moderator:

Tigran Khrimian is Senior Vice President of Enterprise Data Platforms and Business Applications, responsible for technologies that optimize the collection and management of data to maximize its value for FINRA regulatory decision making and Industry compliance. Mr. Khrimian oversees Big Data technology that processes and analyzes as much as 500+ billion market events daily from exchanges, broker-dealers, and other market data sources to reconstruct stock market activity and enable regulatory monitoring of trading practices for potential issues related to compliance or misconduct. Mr. Khrimian is also responsible for digital transformation initiatives that simplify and unify broker-dealers' interactions with FINRA systems to facilitate more efficient and effective firm compliance programs. He oversees technology that handles qualification exams for securities professionals and central licensing and registration for the U.S. securities industry and its regulators. He played a key role in the technology consolidation of NASD and NYSE Regulation as part of the creation of FINRA in 2007. Prior to joining FINRA, Mr. Khrimian was a key member of the technology team at Chessiecap—an arm of an investment banking company specializing in mergers and acquisitions. Prior to his tenure at Chessiecap, he worked at the Adrenaline Group as a software architect, performing rapid software development of commercial products to help startup companies and well-established businesses with their online presence. Mr. Khrimian started his career as a developer at IBM, building software products in support of IBM's business critical operations. He holds a B.S. in Computer Science from the University of Maryland and an M.S. in Computer Science from Johns Hopkins University.

Panelists:

Noah Egorin is senior director and product manager for Business Development & Innovation in FINRA's Credentialing, Registration, Education and Disclosure (CRED) department. He is responsible for leading FINRA's effort to modernize and transform the products the industry utilizes to meet their registration and disclosure obligations. Mr. Egorin is also focused on utilizing FINRA's information, analyses, and unique role to create new products that benefit the financial services industry. Prior to his current role, Mr. Egorin led FINRA's Firm Compliance Tools unit where he focused on developing tools to assist broker-dealers with compliance activities. His efforts have focused on compliance tool offerings associated with variable annuity exams, mutual funds, and municipal bond disclosure. In this role, Mr. Egorin was responsible for the FINRA Report Center (and associated Report Cards), FINRA's Online Manual, and other interactive tools. He has also supported FINRA's efforts to syndicate investor education materials and develop data interfaces for FINRA systems. Prior to joining FINRA, Mr. Egorin served as group manager for the product planning practice of the Adrenaline Group, a Washington, DC-based consulting firm that assisted firms with commercial product development, and also spent time as program manager on the Microsoft Office team in Redmond, WA. Mr. Egorin holds a B.S. in computer science from Washington & Lee University.

Julia McCafferty joined FINRA in 2019 and is currently the Director of Product Management for FINRA's Digital Experience Transformation (DXT). Ms. McCafferty has pursued human-centered product design for 18 years. Although she began her career as a licensed financial representative, she quickly realized her strengths in providing better user experiences in fin-tech and transitioned from business to technology with great ease. Ms. McCafferty has worked for two Fortune 500 companies, The Ohio State University, and three start-ups, always bringing her passion for efficiency and innovation. Most recently, she spent five years at JP Morgan, partnering globally with financial clients optimizing the firms' global digital experience. Ms. McCafferty holds a B.S. in Computer Science Technical Management, and an M.S. in User Experience Design. Ms. McCafferty works out of the Rockville, Maryland office.

Michele Oswald is a team leader in the Compliance Registration department. Her team ensures associates and locations are appropriately registered with regulators while keeping the best interests of clients in mind. They strive to be an industry leader in best practices for compliant, accurate, and efficient registrations in an agile and engaging work environment. Part of her role is to work closely with FINRA on efforts such as the CRD Transformation. She engages with industry peers and FINRA stakeholders to deepen business relationships. Ms. Oswald has been in the securities industry for 17 years. She joined Edward Jones in 2004 as a Records Administrator in the Verification Letters department. In 2006, she joined the Compliance Registration department and has held various roles. Her Edward Jones career has all been within Compliance and predominantly in Compliance Registration. She is a member of The Association of Registration Management, Inc. (ARM) and the Securities and Insurance Licensing Association (SILA). She earned a bachelor's degree in Computer Management Information Systems from Southern Illinois University Edwardsville in 2004.

Jennifer Szaro is Chief Compliance Officer for XML Securities, LLC a fully disclosed introducing broker/dealer and its affiliated investment advisory firm, XML Financial Group. Ms. Szaro is responsible for managing both firms' compliance infrastructures. Ms. Szaro joined the securities industry in 2000. She previously worked in the technology sector where she had experience in ecommerce, website hosting and product development. As the securities industry went through significant changes with higher regulatory demands, she took on more compliance and marketing related roles. In 2011, she became a senior level executive and Chief Compliance Officer of the broker dealer, then dually registered. In addition to her current role as CCO, she is the AMLCO, and alternative FINOP. In 2012, she completed FINRA’s Certified Regulatory and Compliance Professional Program (CRCP)®. In 2018, she became a non-public FINRA Dispute Resolution Arbitrator, having qualified through the National Arbitration and Mediation Committee. In 2019, she was appointed to serve out a two-year term on the FINRA’s Small Firm Advisory Committee (SFAC), serving as the 2020 Chair. She was re-appointed to serve a three-year term through 2023. Ms. Szaro holds the following FINRA registrations; Compliance Officer (CR), Introducing Broker-Dealer Financial and Operations Principal (FI), General Securities Principal (GP), General Securities Representative (GS), Investment Company and Variable Contracts Products Representative (IR), Municipal Securities Principal (MP), Municipal Securities Representative (MR), and Operations Professional (OS). Ms. Szaro is a graduate from the University of Rhode Island with a Bachelor of Science.

Changing Firms Digital Experience

Panelists

- **Moderator**
  - Tigran Khrimian, Senior Vice President, Enterprise Data Platforms & Business Applications, FINRA Technology
- **Panelists**
  - Noah Egorin, Senior Director, Business Development & Innovation, FINRA Credentialing, Registration, Education and Disclosure (CRED)
  - Julia McCafferty, Director, Product Management, FINRA Technology
  - Michele Oswald, Team Leader, Edward Jones
  - Jennifer Szaro, CRCP®, Chief Compliance Officer, XML Securities, LLC

Changing Firms Digital Experience

FINRA has created a culture of innovation and is an industry leader in the use of its technology tools and resources.

- Discuss FINRA's mission to change the digital experience for our member firms.
- Learn about innovative ways FINRA is partnering with the industry to provide the best possible service.

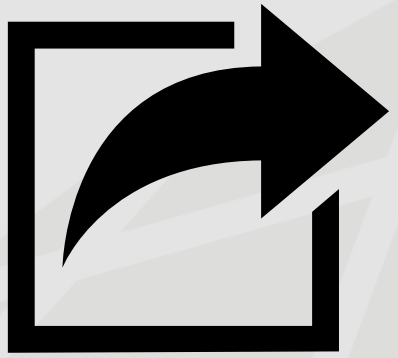
Key Benefits

eSignature

Ability to have reps digitally sign registration documents.

Notifications

Ability to decide when and how to be notified.



Requests & Filings

Ability to locate and respond to tasks and see updated statuses in one place.

Building With Users

FINRA Gateway

1000+ **Industry feedback suggestions** using FINRA Gateway online ticketing

8000+ **Survey responses** received

100+ **new improvements** tied directly to your feedback

Industry Testimonials

Firms estimate18-25% time savings with the new FINRA Gateway

> "... I think today's exchange is the **best form of online customer support I have ever received** in my professional and personal life..."
>
> *- re: Online Ticketing*

> "I LOVE that FINRA is pushing us to have **access to our own data** - I think we truly need to be able to access all of it."
>
> *- re: Dynamic Reporting*

> "I appreciate how **FINRA listens and responds to the customer.**"
>
> *- re: Customer Engagement*

> "**Saved view is so much more improved!** I can search and then easily save my search to get back to my list of work again and again!"
>
> *- re: Requests & Filings*

FINRA Gateway

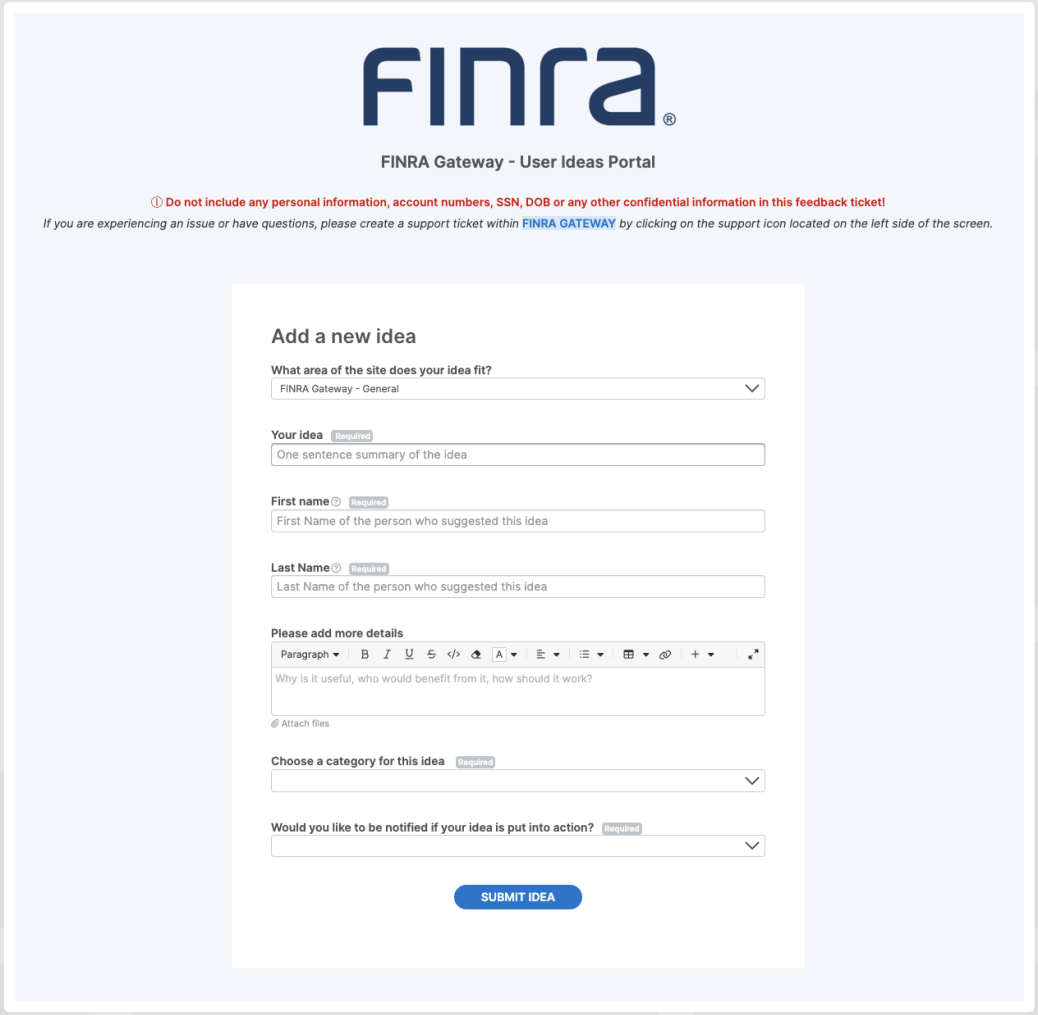
Thank you for your participation in this transformation journey!

Contact Us

Stop by the booth to participate in the **LIVE Feedback collection**

Submit Feedback

FINRA Gateway - User Ideas Portal



Gamification, Mobile Apps and Digital Engagement
Tuesday, May 17, 2022
1:45 p.m. – 2:45 p.m.

Attend this session to hear how regulatory and industry experts are evaluating the rapidly changing world of digital communications and digital engagement practices. Panelists discuss risks and benefits of gamification features on broker-dealers' apps and websites. They address how firms can effectively supervise digital communications.

Moderator:
Amy Sochard
Vice President
FINRA Advertising Regulation

Panelists:
Surabhi Ahmad
Vice President, Compliance
Ameriprise Financial Services, LLC

Alexander Gavis
Professor
Suffolk University Law School

Alicia Goldin
Senior Special Counsel, Office of Chief Counsel, SEC Division of Trading and Markets
U.S. Securities and Exchange Commission (SEC)

Haimera Workie
Vice President, Financial Innovation
FINRA Office of Financial Innovation (OFI)

Gamification, Mobile Apps and Digital Engagement Panelists Bios:

Moderator:

Amy C. Sochard is Vice President of FINRA's Advertising Regulation Department. The department helps protect investors by ensuring members of FINRA use communications including social media, digital advertising and other marketing material that are fair, balanced, and not misleading. Ms. Sochard oversees the department's regulatory review programs and business operations, including the development of technology to facilitate the review of communications. Ms. Sochard provides expertise and policy guidance to other FINRA departments concerning FINRA, SEC, MSRB and SIPC rules pertaining to communications with the public. She also oversees the development of new rules, published guidance, and interpretations regarding communications, and she routinely speaks at industry events on these topics. Prior to joining FINRA, Ms. Sochard worked with a real estate syndication firm in Washington, DC. She received a bachelor's degree with distinction in English from the University of Virginia and studied poetry writing at Columbia University.

Panelists:

Surabhi Ahmad is Vice President, Compliance at Ameriprise Financial. She leads a global team charged with the compliance review of advertising, marketing and communication materials for Ameriprise and its insurance and asset management businesses, RiverSource and Columbia Threadneedle Investments. She also leads a team of compliance professionals supporting the distribution of U.S. and global products for Columbia Threadneedle through intermediary and institutional channels. Based in Boston, Ms. Ahmad joined Ameriprise Financial in 2011. She has spent the last 24 years in risk- and compliance-related roles within the financial services industry including leadership roles at State Street Global Advisors and Fidelity Investments. She has also worked at international firms in Singapore and India supporting clients with trade finance, immigration and corporate law needs. Her diverse and international experience has enabled her to provide a global perspective to the multiple organizations she's been a part of. Ms. Ahmad received a B.S. from Calcutta University and a Professional Law Certification from the Delhi C.S. Institute in India. She holds the Series 7 and Series 24 securities license with FINRA.

Alexander C. Gavis recently retired as Senior Vice President and Deputy General Counsel in the Corporate Legal Department of FMR LLC, the parent company of Fidelity Investments, one of the largest brokerage and mutual fund companies in the United States and the leading provider of workplace retirement savings plans. He managed a team of attorneys and professionals responsible for providing legal services to the firm's retail brokerage, stock plan and workplace retirement businesses. He also managed legal services for Fidelity's businesses involved in electronic and mobile commerce, start-up innovation, and social media. Mr. Gavis provided legal advice on all of Fidelity's national advertising and marketing initiatives. Prior to joining Fidelity in 1997, Mr. Gavis served as Assistant Counsel at the Investment Company Institute and as Senior Counsel in the Office of General Counsel at the U.S. Securities and Exchange Commission, both in Washington, DC. He also served as a judicial law clerk for The Honorable William T. Allen, Chancellor of the Court of Chancery for the State of Delaware. He has worked in investment banking in New York at Salomon Brothers Inc, handling mergers and acquisitions. Mr. Gavis received his J.D., *cum laude*, from the University of Pennsylvania Law School, where he served as Editor-in-Chief of the *University of Pennsylvania Law Review*, and his bachelor's degree, with High Honors and *Phi Beta Kappa,* from Swarthmore College. As an adjunct professor at Suffolk University Law School, he currently teaches the class "Designing Thinking for Lawyers and Business Professionals" and has taught at the Stanford University Design and Law Schools and at Harvard Law School. He also holds a patent in the area of blockchain technologies. Mr. Gavis currently serves on FINRA's FinTech Industry Committee and as chair of the Public Communications Committee, and as a past member of the E-Brokerage (chair) and Membership Committees and the Social Media (chair) and New Account Form Task Forces.

Alicia Goldin is Senior Special Counsel in the Division of Trading and Markets, Office of Chief Counsel, specializing in broker-dealer sales practices, with a particular focus on issues relating to Regulation Best Interest, Form CRS, advertising, supervision and arbitration. Ms. Goldin previously served as Counsel to former SEC Commissioner Elisse B. Walter. Prior to joining the Commission in 2007, Ms. Goldin spent four years in private practice. She earned her law degree from the University of Michigan Law School and her undergraduate degree from the University of Virginia.

Haimera Workie, Vice President and Head of Financial innovation, oversees the Office of Financial Innovation. In this capacity, he is responsible for leading FINRA's Office of Financial Innovation, which focuses on analyzing financial technology (FinTech) innovations and emerging risks and trends related to the securities market. As part of these responsibilities, Mr. Workie works to foster an ongoing dialogue with market participants in order to build a better understanding of FinTech innovations and their impact on the securities markets. Previously, Mr. Workie served as Deputy Associate Director in the Division of Trading and Markets at the U.S. Securities and Exchange Commission. Mr. Workie also previously served as Counsel in the SEC's Office of the Chairman. Prior to joining the SEC, he was an associate at the law firm of Skadden, Arps, Slate, Meagher & Flom, with a practice focusing on corporate law. Mr. Workie is a graduate of the Massachusetts Institute of Technology (B.S., M.S.) and Harvard Law School (J.D.).

Gamification, Mobile Apps and Digital Engagement

Panelists

- **Moderator**
  - Amy Sochard, Vice President, FINRA Advertising Regulation
- **Panelists**
  - Surabhi Ahmad, Vice President, Compliance, Ameriprise Financial Services, LLC
  - Alexander Gavis, Professor, Suffolk University Law School
  - Alicia Goldin, Senior Special Counsel, Office of Chief Counsel, SEC Division of Trading and Markets, U.S. Securities and Exchange Commission (SEC)
  - Haimera Workie, Vice President, Financial Innovation, FINRA Office of Financial Innovation (OFI)

Agenda

01 | Digital Engagement Practices Overview

02 | Mobile App Considerations

03 | Data Analytics

04 | Future Developments

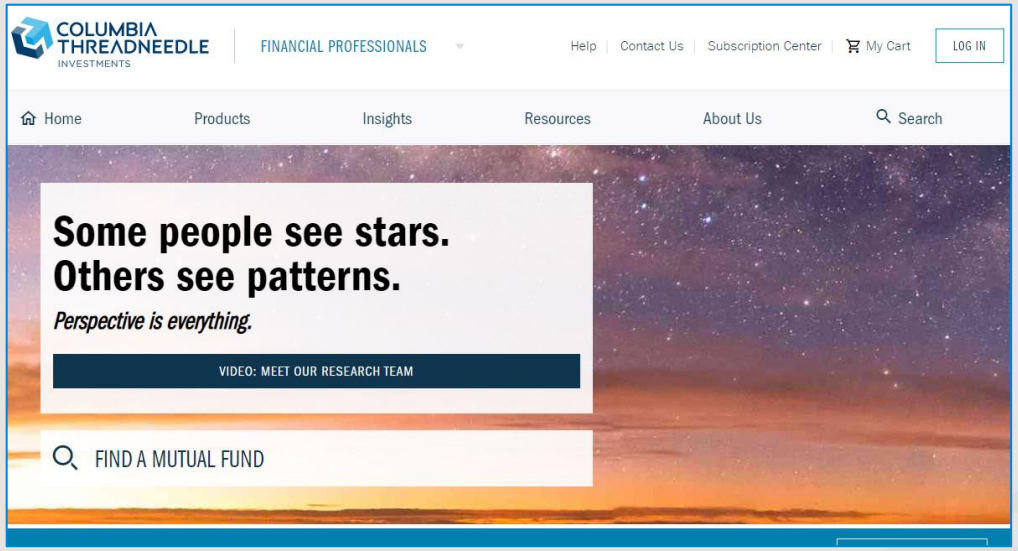
1 Digital Engagement Practices Overview

Digital Engagement Practices Overview

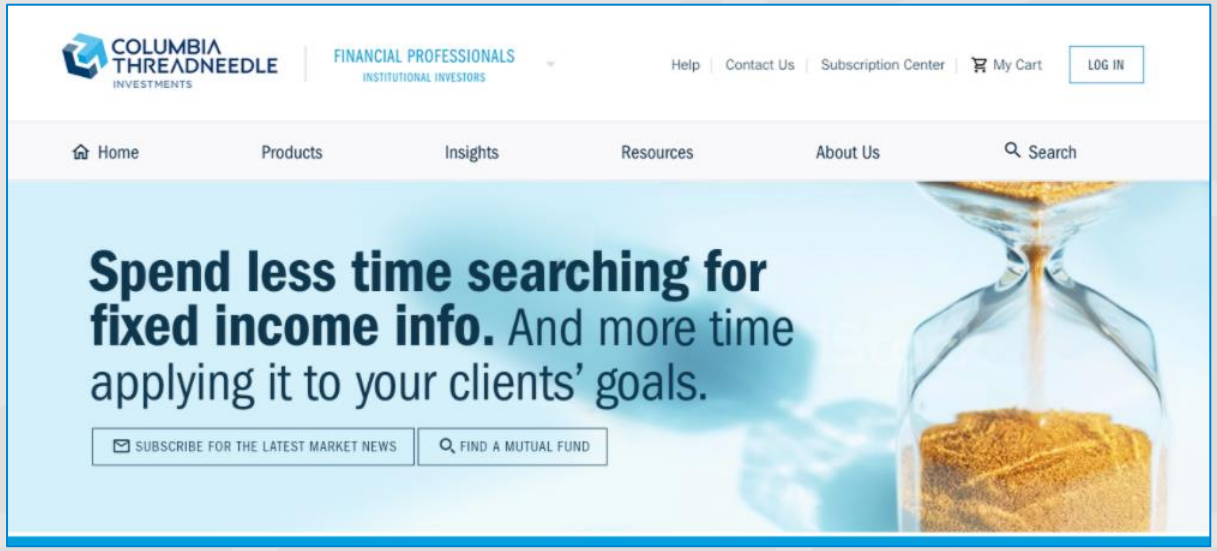
- *SEC Request for Information and Comments on Broker-Dealer and Investment Adviser Digital Engagement Practices, Related Tools, etc.* Release Nos. 34-92766; IA-5833; File No. S7-10-21
- Digital Engagement Practices and Gamification Definitions
- Pros and Cons of Digital Engagement Practices
- Responses to SEC Request
- FINRA Observations

Customizing the Website Experience

From: Static Website

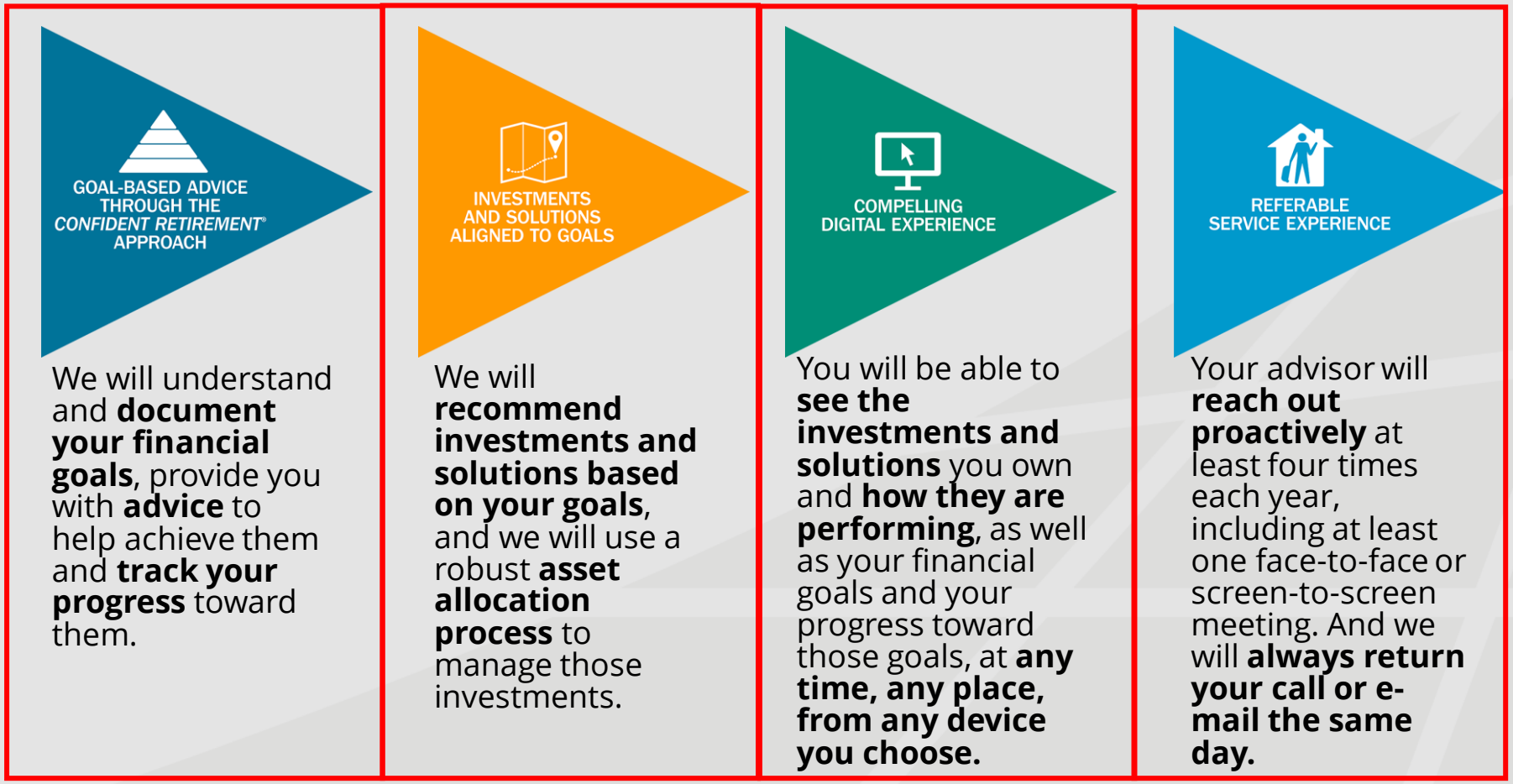


To: Customized Website Experience

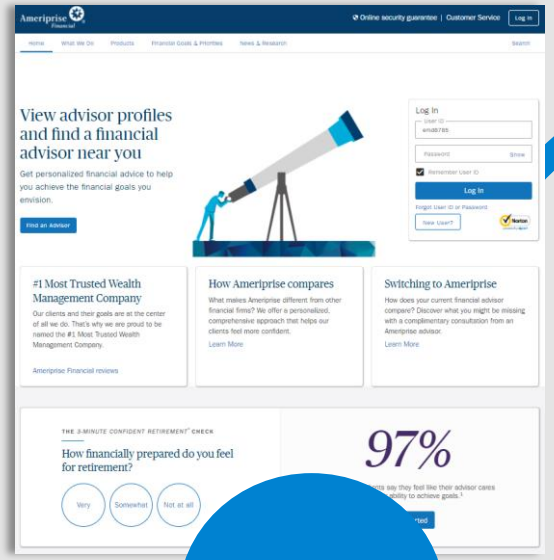


Our digital capabilities and marketing programs support the Ameriprise Client Experience

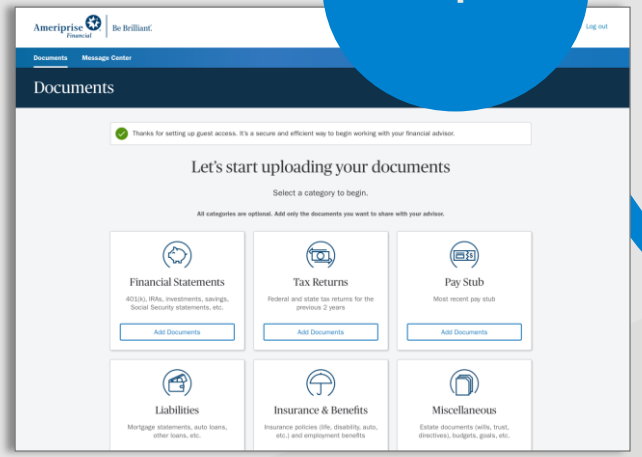
Our **clients' expectations have changed**, especially when it comes to the online client experience. **They want and expect a compelling digital experience** that allows them to **collaborate** with advisors; they want to **see** their investments and performance, as well as their financial goals and their **progress** towards these goals **at any time**, any place, from any device they choose.



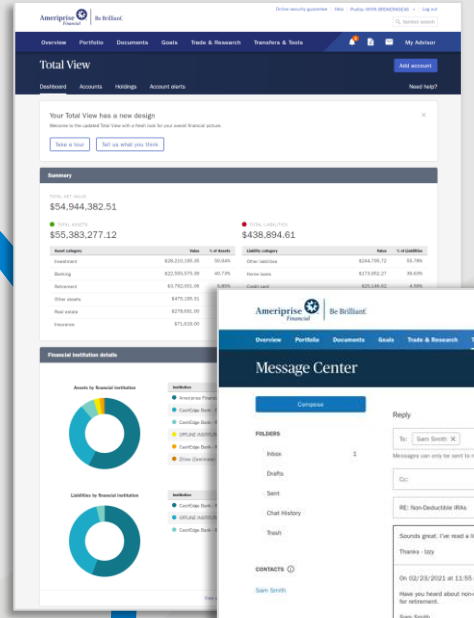
We shape the online experience for prospects and clients

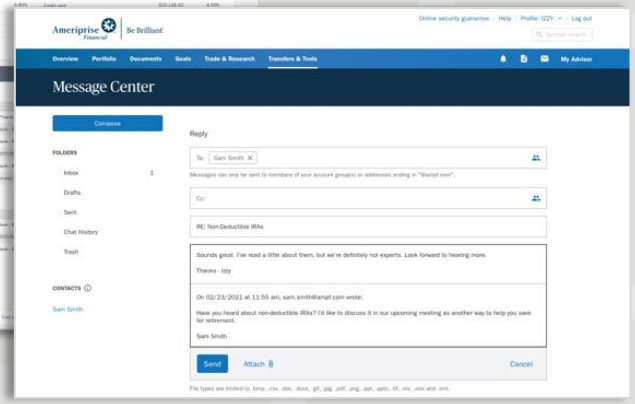


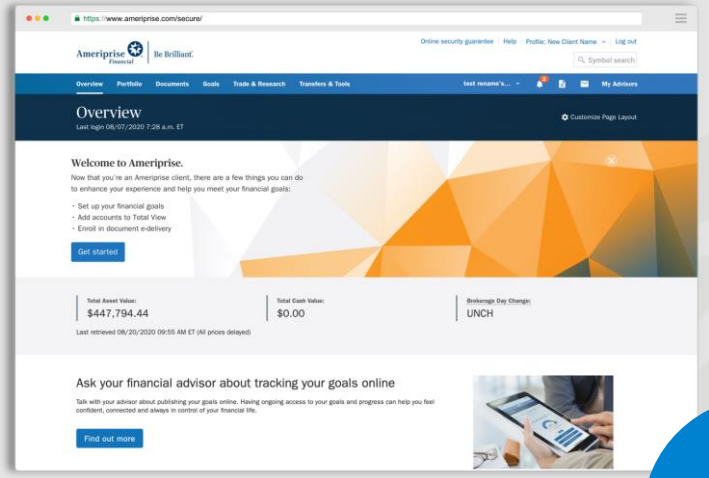
Prospect



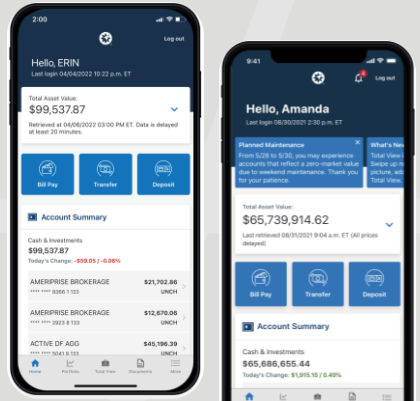
Client/ Advisor







Client Self-Service



2 | Mobile App Considerations

Mobile App Considerations

- *2022 Report on FINRA's Examination and Risk Monitoring Program, Communications with the Public*
- Broker Dealers' Approaches to Use and Marketing of Mobile Apps
- Supervision of Mobile Apps
- Challenges

3 | Data Analytics

Data Analytics

- Regulatory Observations
- Personalization
- Reg BI
- Privacy Considerations

4 | Future Developments

Future Developments

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

Conformed to Federal Register version

SECURITIES AND EXCHANGE COMMISSION

[Release Nos. 34-92766; IA-5833; File No. S7-10-21]

RIN 3235-AN00

Request for Information and Comments on Broker-Dealer and Investment Adviser Digital Engagement Practices, Related Tools and Methods, and Regulatory Considerations and Potential Approaches; Information and Comments on Investment Adviser Use of Technology to Develop and Provide Investment Advice

AGENCY: Securities and Exchange Commission.

ACTION: Request for information and comment.

SUMMARY: The Securities and Exchange Commission (the "Commission" or the "SEC") is requesting information and public comment ("Request") on matters related to: broker-dealer and investment adviser use of "digital engagement practices" or "DEPs", including behavioral prompts, differential marketing, game-like features (commonly referred to as "gamification"), and other design elements or features designed to engage with retail investors on digital platforms (e.g., websites, portals and applications or "apps"), as well as the analytical and technological tools and methods used in connection with these digital engagement practices; and, investment adviser use of technology to develop and provide investment advice. In addition to or in place of responses to questions in this release, retail investors seeking to comment on their experiences may want to submit a short Feedback Flyer.

DATES: Comments should be received on or before October 1, 2021.

ADDRESSES: Comments may be submitted by any of the following methods:

Electronic comments:

- Use the Commission's internet comment form (https://www.sec.gov/rules/submitcomments.htm); or

- Send an email to *rule-comments@sec.gov*. Please include File No. S7-10-21 on the subject line.

Paper comments:

- Send paper comments to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090.

All submissions should refer to File Number S7-10-21. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method of submission. The Commission will post all comments on the Commission's website (*http://www.sec.gov*). Comments are also available for website viewing and printing in the Commission's Public Reference Room, 100 F Street NE, Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. Operating conditions may limit access to the Commission's public reference room. All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make publicly available. Retail investors seeking to comment on their experiences with online trading and investing platforms may want to submit a short Feedback Flyer, available at Appendix A.

Studies, memoranda, or other substantive items may be added by the Commission or staff to the comment file during this Request. A notification of the inclusion in the comment file of any such materials will be made available on the Commission's website. To ensure direct electronic receipt of such notifications, sign up through the "Stay Connected" option at www.sec.gov to receive notifications by email.

FOR FURTHER INFORMATION CONTACT: Division of Trading and Markets, Office of Chief Counsel, at (202)-551-5550 or tradingandmarkets@sec.gov; Division of Investment Management, Investment Adviser Regulation Office at (202) 551-6787 or IArules@sec.gov.

SUPPLEMENTARY INFORMATION: The Commission is requesting information and public comment on matters related to (1) broker-dealer and investment adviser use of digital engagement practices on digital platforms, as well as the analytical and technological tools and methods used in connection with such practices; and (2) investment adviser use of technology to develop and provide investment advice.

I. INTRODUCTION

A. BACKGROUND

With the advent and growth of digital platforms for investing, such as online brokerages and robo-advisers, and more recently, mobile investment apps and portals, broker-dealers and investment advisers (referred to collectively as "firms") have multiplied the opportunities for retail investors to invest and trade in securities. This increased accessibility has been one of the many factors associated with the increase of retail investor participation in U.S. securities markets in recent years.

As discussed in Section II of this Request, firms employ a variety of digital engagement practices when interacting with retail investors through digital platforms. Examples of digital engagement practices include: social networking tools; games, streaks and other contests with prizes; points, badges, and leaderboards; notifications; celebrations for trading; visual cues; ideas presented at order placement and other curated lists or features; subscriptions and membership tiers; and chatbots.

Various analytical and technological tools and methods can underpin the creation and use of these practices, such as predictive data analytics and artificial intelligence/machine learning

("AI/ML") models. Firms may use these tools to analyze the success of specific features and practices at influencing retail investor behavior (e.g., opening new accounts or obtaining additional services, making referrals, increasing engagement with the app, or increasing trading). Based on the results obtained from such AI/ML models and data analytics, firms may tailor the features with which different retail investor segments interact on the firms' digital platforms, or target advertisements to specific investors based on their known behavioral profiles.

As discussed in Section III of this Request, some investment advisers also use these tools to develop and provide investment advice, including through online platforms or as part of more traditional investment advisory services. Investment advisers can use analytical tools to learn more about their clients and develop and provide investment advice based on that information. These developments may provide potential benefits and risks for investment advisers and their clients.

B. PURPOSE OF REQUEST

The Commission is issuing this Request related to the use and development of digital engagement practices by firms on their digital platforms, in order to:

1. Assist the Commission and its staff in better understanding and assessing the market practices associated with the use of DEPs by firms, including: (1) the extent to which firms use DEPs; (2) the types of DEPs most frequently used; (3) the tools and methods used to develop and implement DEPs; and (4) information pertaining to retail investor engagement with DEPs, including any data related to investor demographics, trading behaviors, and investment performance.
2. Provide a forum for market participants (including investors), and other interested parties to share their perspectives on the use of DEPs and the related tools and methods,

including potential benefits that DEPs provide to retail investors, as well as potential investor protection concerns.[1]

3. Facilitate an assessment by the Commission and its staff of existing regulations and consideration of whether regulatory action may be needed to further the Commission's mission including protecting investors and maintaining fair, orderly, and efficient markets in connection with firms' use of DEPs and related tools and methods.

In addition to addressing the questions below, the Commission encourages commenters to provide or identify any data and other information in furtherance of the purposes articulated in this Request.

II. DIGITAL ENGAGEMENT PRACTICES, RELATED TOOLS AND METHODS, AND REGULATORY CONSIDERATIONS AND POTENTIAL APPROACHES

A. DEPS

The Commission is issuing this Request, in part, to develop a better understanding of the market practices associated with firms' use of DEPs, which broadly include behavioral prompts, differential marketing, game-like features, and other design elements or features designed to engage retail investors. The Commission is aware of a variety of DEPs that may be used by firms, including the following:[2]

---

[1] To further enable retail investors to share their perspectives, the Commission is issuing a user-friendly "Feedback Flyer." The Commission has determined that this usage is in the public interest and will protect investors, and therefore is not subject to the requirements of the Paperwork Reduction Act of 1995. See Sections 19(e) and (f) of the Securities Act of 1933 ("Securities Act"), 15 U.S.C. 77s(e) and (f). Additionally, for the purpose of developing and considering any potential rules relating to this rulemaking, the agency may gather from and communicate with investors or other members from the public. See Securities Act section 19(e)(1) and (f), 15 U.S.C. 77s(e)(1) and (f).

[2] Broker-dealers' and investment advisers' use of DEPs and the related tools and methods must comply with existing rules and regulations. By identifying observed practices and soliciting comment on them, the Commission is not expressing a view as to the legality or

- Social Networking Tools. Digital platforms may be linked to internet content, enabling users to access social sentiment on the platform. Some digital platforms may embed social networking tools into their platforms, or enhance existing tools to allow an investor to create an on-line persona or avatar. Certain digital platforms enable investors to copy the trades of other investors (known as "copy trading") in certain types of investments.[3]
- Games, Streaks and Other Contests with Prizes. Some digital platforms may employ games that use interactive graphics and offer prizes (e.g., slot-machine style interactive graphics, interactive wheels of fortune, or virtual "scratch-off" lottery tickets), for example, in connection with account opening. Some digital platforms may offer prizes to investors for completing certain "to-do lists" or tasks frequently within a specified time period (known as "streaks") or for other types of contests (including performance-based contests). Prizes may include free stock, cash, gaining access to additional features on the platforms, or a free trial period for a subscription to certain market data or levels of service. Tasks that may generate awards include referring others to the platform, engaging in community forums, linking a bank account, funding an account, trading, or promoting the app on social media.
- Points, Badges, and Leaderboards. Some digital platforms may use points or similar "scorekeeping" related to a specific area of activity. For example, some platforms offer "paper trading" (i.e., simulated trading) competitions that enable investors to practice

---

conformity of such practices with the federal securities laws and the rules and regulations thereunder, nor with the rules of self-regulatory organizations ("SROs").

[3] It is our understanding that copy trading is currently offered in certain investments, such as cryptocurrencies, in the U.S. and may be offered more broadly in other jurisdictions. Copy trading in securities may raise regulatory concerns under the U.S. federal securities laws, including potential broker-dealer and investment adviser status issues.

trading without real money. Certain platforms also offer badges as visual markers of achievement as well as leaderboards to rank individuals based on performance-based criteria developed by the firm.

- Notifications. Some digital platforms may use notifications via email, text, or other means (e.g., push notifications on mobile devices). In some cases, investors can opt-in or opt-out of notifications; in others, notifications may be set by default with no ability to opt-out. Investors may receive notifications indicating a certain stock is up or down, noting a list of stocks qualifying as top "movers" (i.e., largest percentage change in price), or reminding them that it has been a certain number of days since they last engaged in a trade. Notifications may also be used to attempt to reassure investors during periods of market volatility.
- Celebrations for Trading. Some digital platforms may have embedded animations and graphics, such as digital confetti or crowds applauding, that "celebrate" when investors enter orders to purchase stock or options.
- Visual Cues. Interface design elements may provide visual cues, including by displaying certain information more prominently than other information. In some cases, visual cues are targeted specifically to the investor. For example, some digital platforms' user interfaces shift the coloration of the entire screen between green and red based on an investor's portfolio performance. Some digital platforms present relevant news or other pieces of information to the user immediately once the portfolio turns negative.
- Ideas Presented at Order Placement and Other Curated Lists or Features. Some digital platforms may present "ideas" prior to allowing the investor to place an order. These ideas may involve curated lists or features, news headlines, etc.

- Subscriptions and Membership Tiers. Some firms may offer subscriptions or tiered memberships. Examples of additional features that may be provided include access to research reports, briefs, webcasts, and newspaper subscriptions; invitations to sports and industry events; credit line access; and an exemption or reduction of fees. In some cases, investors may be upgraded automatically based on balances and holdings reaching certain thresholds. Some firms may offer free subscription trials.
- Chatbots. Some digital platforms may offer chatbots, or computer programs that simulate live, human conversation. Chatbots may be offered to respond to investor inquiries relating to stock prices, account information, or customer service matters.

DEPs may be designed to encourage account opening, account funding, and trading, or may be designed solely to increase investor engagement with investing apps, as there may be value in the number of investors interacting with the platform, how often they visit, and how long they stay.

The use of DEPs carries both potential benefits and risks for retail investors. Simplified user interfaces and game-like features have been credited with making investment platforms more accessible to retail investors (in particular, younger retail investors),[4] and assisting in the

[4] See, e.g., Evie Liu, The Stock Market is Attracting New Investors. Here Are 3 Trends to Know., Barron's (Apr. 13, 2021), https://www.barrons.com/articles/the-stock-market-is-attracting-new-investors-here-are-3-trends-to-know-51618273799; Broadridge, Insights on the U.S. Investor (2020) ("Zero commission trades, mobile trading applications and the ability to acquire fractional shares are making it more attractive and easier for younger, lower asset investors to trade securities. This is bolstering Millennials' ability to participate more actively in equity investing."); Maggie Fitzgerald, Now Teenagers Can Trade Stocks With Fidelity's New Youth Investing Accounts, CNBC (May 18, 2021), https://www.cnbc.com/2021/05/18/now-teenagers-can-trade-stocks-with-fidelitys-new-youth-investing-accounts.html?&qsearchterm=margin%20debits ("Of the 4.1 million new accounts that Fidelity added in the first quarter of 2021, 1.6 million were opened by retail investors 35 and younger, an increase of more than 222% from a year prior."); Jennifer Sor, Young Investors Drive Increased Use of Investing Apps, Los Angeles Business Journal (Aug. 3, 2020),

development and implementation of investor education tools. Others have noted that DEPs can encourage retail investors to increase their contributions to retirement accounts and to engage in other activities that are traditionally viewed as wealth-building exercises.[5]

On the other hand, DEPs can potentially harm retail investors if they prompt them to engage in trading activities that may not be consistent with their investment goals or risk tolerance. Some have expressed concerns that DEPs encourage: (1) frequent trading;[6] (2) using trading strategies that carry additional risk (e.g., options trading and trading on margin); and (3)

---

https://labusinessjournal.com/news/2020/aug/03/young-investors-drive-increased-use-investing-apps/.

5 See, e.g., Chris Carosa, Are You Ready to Play the 401(k) Game? Hint: You Already Are, Forbes (Apr. 14, 2021), https://www.forbes.com/sites/chriscarosa/2021/04/14/are-you-ready-to-play-the-401k-game-hint-you-already-are/?sh=4d6e1b8674ab; Greg Iacurci, MassMutual Turns to Video Games to Boost Retirement Savings, Investment News (July 18, 2016), https://www.investmentnews.com/massmutual-turns-to-video-games-to-boost-retirement-savings-66476.

6 Some have argued that certain compensation practices (such as payment for order flow or "PFOF," in combination with zero commissions) create incentives for firms to use DEPs to encourage frequent trading, and that these incentives may not be transparent to retail investors. See, e.g., Game Stopped? Who Wins and Loses When Short Sellers, Social Media, and Retail Investors Collide, Part II: Hearing Before the H. Comm. on Fin. Servs., 113th Cong. (2021) (statement of Vicki L. Bogan, Associate Professor, Cornell University), https://docs.house.gov/meetings/BA/BA00/20210317/111355/HHRG-117-BA00-Wstate-BoganV-20210317.pdf. One form of PFOF is a practice wherein wholesale broker-dealers (often referred to as "principal trading firms" or "electronic market makers") offer payment to retail broker-dealers in exchange for the right to trade principally with (or "internalize") their customer order flow. See 17 CFR 10b-10(d)(8). Although PFOF is not prohibited, a broker-dealer must not allow PFOF to interfere with its efforts to obtain best execution for its customers' transactions. See Payment for Order Flow, Securities Exchange Act of 1934 ("Exchange Act") Release No. 34902 (Oct. 27, 1994) [59 FR 55006, at 55009 & n.28 (Nov. 2, 1994)]; see also Robinhood Financial, LLC, Exchange Act Release No. 90694 (Dec. 17, 2020) (settled order) (the Commission brought an enforcement action against a broker-dealer for willfully violating Sections 17(a)(2) and 17(a)(3) of the Securities Act and Section 17(a) of the Exchange Act and Rule 17a-4 thereunder, for, among other things, failing to take appropriate steps to assess whether its higher PFOF rates were adversely affecting customer execution prices).

trading in complex securities products.[7] DEPs also may employ what some researchers have called "dark patterns," described as user interface design choices that are knowingly designed to "confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions."[8]

In the questions below, the Commission's request for comment pertains to all DEPs on brokerage and advisory digital platforms, including, but not limited to, those identified above.

Industry practices:

1.1 What types of DEPs do firms use (or in the future expect to use) on digital platforms and what are the intended purposes of each type of DEP used? For example, are particular DEPs designed to encourage or discourage particular investor actions or behaviors, such as opening of accounts, funding of accounts, trading, or increasing engagement with the app or platform? To what extent and how are firms using DEPs

---

7 In congressional hearings related to market events in January 2021, investor protection concerns were identified relating to the use of certain types of DEPs, including advertisements targeted towards specific groups of investors on digital platforms and game-like features on mobile apps. See Game Stopped? Who Wins and Loses When Short Sellers, Social Media, and Retail Investors Collide: Hearing Before the H. Comm. on Fin. Servs., 113th Cong. (2021), https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=407107; Game Stopped? Who Wins and Loses When Short Sellers, Social Media, and Retail Investors Collide, Part II: Hearing Before the H. Comm. on Fin. Servs., 113th Cong. (2021), https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=406268; Game Stopped? Who Wins and Loses When Short Sellers, Social Media, and Retail Investors Collide, Part III: Hearing Before the H. Comm. on Fin. Servs., 113th Cong. (2021), https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=407748; Who Wins on Wall Street? GameStop, Robinhood, and the State of Retail Investing: Hearing Before the S. Comm. On Banking, Hous., & Urban Affairs, 113th Cong. (2021), https://www.banking.senate.gov/hearings/who-wins-on-wall-street-gamestop-robinhood-and-the-state-of-retail-investing.

8 See Jamie Luguri and Lior Jacob Strahilevitz, Shining a Light on Dark Patterns, 13 Journal of Legal Analysis 43 (2021), https://academic.oup.com/jla/article/13/1/43/6180579.

such as notifications (e.g., push notifications or text messages) or other design elements and features (e.g., design aesthetics in the user interface) as a means to alter (or nudge[9]) retail investor behavior or otherwise to encourage or discourage certain behaviors or activities? If so, what types of design elements are used and how are they used? Please explain any such specific design elements, how they intend to encourage specific retail investor behaviors, and whether and to what extent they are achieving their intended purposes.

1.2 To what extent do firms that utilize DEPs provide retail investors the ability to opt in or out of interacting with those DEPs when using the firm's digital platform? To what extent, and how, are firms tailoring or personalizing DEPs to a particular retail investor?

1.3 What types of firms use DEPs on their digital platforms, and on what types of platforms? Are these practices more prevalent among certain types of firms, or on certain types of platforms? How prevalent is the use of DEPs by broker-dealers? How prevalent is the use of DEPs by investment advisers? Which types of DEPs are most prevalent? For firms that have chosen not to use DEPs or certain DEPs, what are their reasons? Are firms that are not currently using DEPs considering adopting such features in the future?

1.4 What market forces are driving the adoption of DEPs on digital platforms and how? For example, to what extent and how is the use of DEPs influenced or driven by

---

[9] Richard Thaler and Cass Sunstein define "nudge" as "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives." See Richard H. Thaler and Cass R. Sunstein, Nudge: Improving Decisions About Health, Wealth, and Happiness 6 (Penguin Books 2009).

market practices related to compensation and revenue (e.g., "zero commission" and PFOF)? What types of compensation and revenue arrangements influence or drive market practices related to the use of DEPs? Do such arrangements vary across product types and asset classes (e.g., options, other complex products)? How does the competition for new customers or clients or the retention of existing customers or clients drive firm adoption or use of DEPs?

1.5 Are DEPs used to promote or otherwise direct retail investors to specific securities or certain types of securities, investment strategies, or services? If so, what types of securities, investment strategies, and services, what types of DEPs are used, and how are the DEPs used for these purposes? Do firms use DEPs to promote or otherwise direct retail investors to securities, investment strategies, or services that are more lucrative for the firm or that may be riskier to the retail investor than others – such as: margin services, options trading, proprietary products, products for which the firm receives revenue sharing or other third-party payments, or other higher fee products? Do firms use DEPs that are or can be tailored to the retail investor's investment profile and risk tolerance? If so, how? If not, why not?

1.6 To what extent and how do firms monitor the use and proper functioning of DEPs? For example, to what extent and how do firms monitor notifications that retail investors receive or see from or on the firm's digital platforms?

1.7 To what extent and how do firms use DEPs or alter their use of DEPs in response to changes in the market price volatility and trading volumes in securities, both for specific assets and the market as a whole? For example, to what extent and how do firms use DEPs to notify retail investors of market events? To what extent and how

do firms use DEPs to notify retail investors of firm policies and procedures or other actions that may be taken by the firm, such as in response to market events (e.g., imposition of trading restrictions)? What type of DEPs are used, what information is communicated through DEPs in such circumstances, and what is the timing of such communications?

1.8 Are firms seeking to use DEPs specifically to increase investor education? If so, how? What type of investor educational content is provided, how is that content chosen, and what types of DEPs are used? For example, are firms using DEPs to educate investors about the risks of certain activities, such as trading on margin or options trading? Are firms using DEPs to help investors understand how to make investment choices that are consistent with their investment objectives? If so, what types of DEPs are they using for these purposes, and how are they used? Have firms tested or otherwise observed the effectiveness of any such educational efforts at increasing retail investor knowledge and understanding of investing concepts including risks? Please explain and include any relevant data or information.

1.9 Do firms use DEPs to encourage longer-term investment activities, including, but not limited to, increased contributions to or establishment of retirement accounts? If so, how?

1.10 Do firms that utilize DEPs offer live, phone-based customer support or customer support through live, human-directed online support (i.e., online conversations that are not through an automated chatbot)? Does the availability of this type of support depend on the type of account or investments held (e.g., investors holding riskier products) or on account balances or asset thresholds? If firms offer live, phone-based

customer support or human-directed online support, what training do firms offer their customer support personnel, and what monitoring and quality assurance programs are used? How do firms interact with investors when the platform is unavailable--for example, when the firm has lost internet service or when the platform is undergoing maintenance? What alternative means of communication are available to investors during those times?

1.11 To what extent and how do firms target certain specific groups of retail investors (including prospective customers or clients) through DEPs? What types of DEPs are used, and how are they targeted to specific retail investors or groups of retail investors? What factors do firms look to when deciding which groups of retail investors to target for each type of DEP?

1.12 What feedback, positive or negative, or complaints do firms receive from retail investors relating to the use of DEPs?

Investor characteristics and practices:

1.13 What types of retail investors are customers or clients of firms that utilize DEPs? How does this customer or client base differ, if at all, from those firms that do not use such features—including as to age, prior investment experience, education, net worth, risk tolerance, liquidity needs, investment time horizon, and investment objectives? What types of retail investors engage most frequently with DEPs on platforms that use them? Do firms utilize DEPs for only certain types of customers or clients? If so, which ones and why? To what extent and how have DEPs enabled firms to reach, educate, and provide experience to first-time retail investors? To what extent and how have DEPs enabled retail investors to access specific investments or investment

strategies more quickly and/or with less investing experience than under traditional methods? Please provide or identify any relevant data and other information.

1.14 What trading or investment activities are retail investors engaging in through digital platforms that use DEPs? For retail investors who were investing prior to using digital platforms that use DEPs, how have their activities with respect to trading and investing changed since they started using such platforms and/or were first exposed to DEPs? For example, how often do retail investors engage in trading or investing through such platforms, how often did they engage in trading or investing prior to using such platforms, and how has such frequency changed as a result of using such platforms and/or being exposed to DEPs? How often do retail investors engage in other ways with such platforms (e.g., education, social features, and games)? How do retail investors learn of these platforms (e.g., news coverage, social media, internet search, paid advertisements)? Do firms collect data on how retail investors learn about or use the platforms, such as by asking as part of account opening? Please provide or identify any relevant data and other information.

1.15 What customer and client trends have been observed in connection with or as a result of the adoption and implementation of DEPs? Specifically, is data available regarding changes in customer or client behavior, including in accounts opened, amount invested, frequency of deposits, order frequency, order size (including fractional shares), types of securities traded, the risk profiles of securities that are traded, use of margin, volume of customer complaints, and the adoption and use of new features on the firms' digital platforms? Is there data showing how, for customers with a similar investment profile, these changes compare with any changes

in the behavior of customers or clients of firms that do not utilize DEPs? Is there data regarding numbers or percentages of new accounts opened by retail investors that received targeted communications from the firm as compared to new accounts opened by retail investors that had received no prior communications from the firm? Please provide or identify any relevant data and other information. What experience did retail investors have in the market prior to interacting with DEPs? What percentage of retail investors invested for the first time after interacting with a DEP? What role did DEPs play in their decision to begin investing?

Public perspectives and data:

1.16 What are the benefits associated with the use of DEPs from the perspective of firms, retail investors, and other interested parties? How do these benefits differ depending upon the type of feature used? Are there specific types of DEPs or specific uses of DEPs that have the potential to be particularly beneficial to retail investors? Are there significant investor protection benefits that arise from the use of DEPs generally or particular DEPs? Which particular DEPs and why? Are there ways in which DEPs are particularly successful at conveying information to retail investors in a way that they can process and implement effectively? Please provide or identify any relevant data and other information.

1.17 What are the risks and costs associated with the use of DEPs from the perspective of firms, retail investors, and other interested parties? How do these risks or costs differ depending upon the type of feature used? Are there significant investor protection concerns that arise from the use of DEPs generally or particular DEPs? Are there particular DEPs that may pose unique risks or elevated investor protection concerns? Are there characteristics of particular DEPs that may encourage retail investors to

engage in more frequent trading or invest in higher risk products or strategies? Please provide or identify any relevant data and other information.

1.18 What experience do retail investors have with DEPs? Do retail investors believe that DEPs have caused a change in their investing behavior or type of investments? If so, how? Do retail investors feel like DEPs help or hurt their overall investment performance? Do retail investors believe DEPs have helped increase their understanding of securities markets and investing? If so, how? Do retail investors believe DEPs have made trading, investing, and monitoring their investments more or less accessible to them? Do retail investors believe DEPs have increased or decreased the benefits or risks of trading or investing in securities products? Do retail investors believe that they would have invested in the markets if only more traditional methods were available? Do retail investors believe that they would trade less frequently, invest in different products, or use different investment strategies if only more traditional methods were available?

1.19 Do retail investors believe they are receiving investment advice or recommendations from DEPs or certain types of DEPs? If so, please explain. What types of DEPs do retail investors believe are most beneficial, and what types of features are most harmful, in meeting their own trading or investment objectives?

1.20 For retail investors who have previously invested with the assistance of a financial professional, how do they believe their investing experience has changed as a result of interacting with a digital platform as opposed to a financial professional?

1.21 How do commenters view the educational services currently provided by digital platforms? How could firms adopt or modify DEPs to facilitate and increase

opportunities for investor education and encourage longer-term investment activities, including, but not limited to, through increased contributions to or establishment of retirement accounts?

1.22 What similarities and differences exist between the functionality, and overall user experience, including with respect to DEPs, on a digital trading or investment platform versus similar practices on digital platforms in other contexts (e.g., shopping, fitness, entertainment)? Does a retail investor's experience with these types of features in other contexts affect the retail investor's trading or investment activity, and their engagement with the broker-dealer or investment adviser's digital platform where DEPs are employed? Do commenters believe that certain types of DEPs are more, less, or as appropriate in the investing context than in other contexts? What types of features and why?

1.23 Have researchers (including in the fields of behavioral finance, economics, psychology, marketing, and other related fields) studied the use of DEPs by broker-dealers and investment advisers? In particular, how have these practices been studied or observed to influence or reinforce the behavior of retail investors? To the extent retail investors have shifted from investing through human interaction (with a financial professional) to digital interaction (on a digital platform), how has that shift affected the behavior of retail investors? Please identify any relevant literature or data, including research related to the use of similar practices in other fields that could assist the Commission in its consideration of these issues.

1.24 Is there research in the fields of experimental psychology and marketing that contains evidence regarding the ability of DEPs to influence retail investors? Are there

findings in those fields that suggest retail investors may not be fully aware that they have been influenced by a particular DEP?

1.25 Do studies of gambling or addiction offer evidence regarding whether and to what extent the immediate positive feedback provided by certain DEPs may influence retail investor decision-making?

1.26 How do commenters view the disclosures that firms are providing in connection with or specifically addressing the use of DEPs and the timing of such disclosures? In particular, how effective are disclosures at informing retail investors of any associated conflicts of interest presented by the use of DEPs and how DEPs could influence them and their trading and investing behavior? How accessible are these disclosures to retail investors engaging with DEPs? Please identify any relevant data or other information.

B. DEP-RELATED TOOLS AND METHODS

In order to develop, test, and implement these practices, and thereafter to assess their effectiveness, firms may use numerous analytical and technological tools and methods.[10] From a technological perspective, these tools and methods can employ predictive data analytics and AI/ML models—including deep learning, supervised learning, unsupervised learning, and reinforcement learning processes.[11] These tools and methods can be designed to build and adapt

---

[10] In some cases, firms may rely on in-house and proprietary tools and methods to develop, test and implement DEPs, and in others, firms may use third-party service providers to assist in the DEP development process.

[11] See, e.g., Department of the Treasury et al., Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning (Feb. 2021) [86 FR 16837, 16839-40 (Mar. 31, 2021)] ("Treasury RFI"); FINRA, Artificial Intelligence (AI) in the Securities Industry 5 (June 2020) ("FINRA AI Report"), https://www.finra.org/sites/default/files/2020-06/ai-report-061020.pdf; Financial Stability

DEPs based on observable investor activities. Such adaptations may be based on the AI/ML models' understanding of the neurological rewards systems of retail investors (obtained in the interactions between each retail investor and the firm's investment platform), and may be utilized to develop investor-specific changes to each retail investor's user experience.

Relatedly, firms that utilize AI/ML models may utilize model risk management to provide a governance framework for these models throughout their life cycle in order to account for AI/ML-specific risks. Technological tools and methods also include the use of natural language processing ("NLP") and natural language generation ("NLG"). These specific uses of AI/ML may be employed to transform user interfaces and the interactions that retail investors have on digital platforms by developing an understanding of the investor's preferences and adapting the interface and related prompts to appeal to those preferences.[12]

Beyond technological tools, firms may engage in various forms of research in order to help shape the DEPs developed and implemented on their platforms. This may include consultations with behavioral science professionals, and cross-industry research intended to identify those customer engagement practices used in other industries that have proven most effective.

Industry practices:

2.1 To what extent, and how, do firms use (or in the future expect to use) tools based on AI/ML (including deep learning, supervised learning, unsupervised learning, and

---

Board, Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications (Nov. 1, 2017) ("FSB AI Report"), https://www.fsb.org/wp-content/uploads/P011117.pdf.

[12] See, e.g., FSB AI Report, supra note 11, at 14-15 (finding that chatbots are being introduced by a range of financial services firms, often in mobile apps or social media, and that chatbots are "increasingly moving toward giving advice and prompting customers to act").

reinforcement learning) and NLP and NLG, to develop and evolve DEPs? What are the objective functions of AI/ML models (e.g. revenue generation)? What are the inputs relied on by those AI/ML models (e.g. visual cues or feedback)? Does the ability to collect individual-specific data impact the effectiveness of the ML model in maximizing its objective functions?

2.2 To what extent, and how, do firms use (or in the future expect to use) behavioral psychology to develop and evolve platforms or DEPs? To what extent, and how, do firms use (or in the future expect to use) predictive data analytics to develop and evolve DEPs? To what extent, and how, do firms use "dark patterns"[13] in connection with DEPs? To what extent do firms utilize these types of tools, analytics, and methods to modify DEPs over time, tailored to a specific retail investor's history on the platform? Which types of tools and methods are used for these and other purposes?

2.3 What types of research, information, data, and metrics are firms collecting, acquiring, and using in connection with the tools and methods identified above, or otherwise to design, implement, and modify DEPs and to assess their effectiveness? What are the sources for such information and data (e.g., proprietary research, user data, third-party behavioral research, consultants, other service providers)? Does this research, information, data, and metrics, indicate whether DEPs affect trading frequency, volume, and results? If so, how?

2.4 How are firms using cross-industry research and sources to design, implement, and modify DEPs? Specifically, how are firms using techniques employed, and lessons

[13] See supra note 8.

learned, within industries like retail shopping, video gaming, and video or music streaming services? What features originally adopted in other industries have been utilized and implemented by firms to increase user engagement? How has the use of such features impacted investor activity on digital platforms?

2.5 To what extent, and how, do firms test or otherwise assess how their DEPs affect investor behavior and investing outcomes? What metrics are used for these assessments? What data and other results have such tests and assessments yielded? Have firms found that DEPs can be developed, evolved and implemented in order to affect retail investors' trading or investment behavior, either individually or as a group? Have firms found that those behaviors can be affected in a statistically significant way? If so, how? What controls do firms have in place to monitor the impact of DEPs on investor outcomes? How do firms incorporate any testing and monitoring into their policies and procedures?

2.6 How do firms develop, test, deploy, monitor, and oversee the tools and methods they use, including any AI/ML models (including deep learning, supervised learning, unsupervised learning, and reinforcement learning), NLP, NLG, or other types of artificial intelligence? To what extent are these tools and methods proprietary to firms or offered by third parties? Do relationships with vendors result in conflicts of interest, and if so, what types of conflicts of interest? For example, are broker-dealers or investment advisers affiliated with these providers, or does compensation of the provider vary based upon investor activity? What formal governance mechanisms do firms have in place for oversight of the vendors they use for these purposes? What

model risk management steps do firms undertake? How do firms incorporate these practices and mechanisms into their policies and procedures?

2.7 What type of data concerning retail investors is used to develop, evolve, implement, test and run DEPs? How is this data used? For example, are firms using data on how retail investors—individually and/or when grouped together—have engaged with their digital platform (including trading or investment activity) following exposure to DEPs? If so, how? Are firms tailoring or personalizing DEPs to individual retail investors or groups (or sub-groups) of retail investors? If so, how? Are firms collecting information about specific identifiers attributable to particular retail investors or groups (or sub-groups) of retail investors? If so, what types of specific identifiers are collected? Do firms use such identifiers (or others) in connection with determining the location of retail investors? If so, how do firms use location information? Do firms seek to cause any particular types of engagement with DEPs? If so, how? Are there other ways firms are using data concerning retail investors to develop, evolve, implement, test, and run DEPs?

2.8 To what extent do firms purchase data from third-party vendors, including data concerning retail investors, to develop, evolve, implement, test, and run DEPs? How are firms utilizing data acquired from third-party vendors to develop, evolve, implement, test, and run DEPs? Are firms using data obtained from third-party vendors to tailor or personalize DEPs to individual retail investors? If so, how? To what extent do firms sell or otherwise share data about their own customers' or clients' behavior on their digital platforms, and who are the primary purchasers or recipients of that data?

2.9 To the extent that firms use AI/ML to develop, evolve, implement, test, and run DEPs, are they ensuring that the AI/ML is explainable and reproducible?[14] If so, how?

2.10 Are there any particular challenges or risks that firms face in using AI/ML (including deep learning, supervised learning, unsupervised learning, and reinforcement learning), including AI developed or provided by third parties? If so, what are they and how do firms address such challenges or impediments and any risks associated with them? Have firms found that using AI/ML or retail investor data gathered in connection with DEPs raises unique issues related to financial privacy, information security, or identity theft prevention?

2.11 To what extent and how do firms employ controls to identify and mitigate any biases or disparities that may be perpetuated by the use of AI/ML models[15] in connection

---

[14] See, e.g., Treasury RFI, at 16839-40 (describing explainability as "how an AI approach uses inputs to produce outputs" and describing challenges associated with lack of explainability); see also FSB AI Report, at 2 (stating that the "lack of interpretability or 'auditability' of AI and machine learning models could become a macro-level risk"); Gregory Barber, Artificial Intelligence Confronts a 'Reproducibility' Crisis, Wired (Sept. 16, 2019), https://www.wired.com/story/artificial-intelligence-confronts-reproducibility-crisis/.

[15] See e.g., Joy Buolamwini and Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proceedings of Machine Learning Research 77 (2018), https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf; Ziad Obermeyer et al., Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations, 366 Science 6464, 447-453 (Oct. 25, 2019), https://science.sciencemag.org/content/366/6464/447; Executive Office of the President of the United States, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights pp. 6-10 (May 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

with the use of DEPs? For example, do firms evaluate the outputs of their AI/ML models to identify and mitigate biases that would raise investor protection concerns? Do firms utilize human oversight to identify biases that would raise investor protection concerns, in both the initial coding of AI/ML models and the resulting outputs of those models?

Public perspectives and data:

2.12 What are the benefits associated with the use of the tools and methods identified above (e.g., AI/ML, predictive data analytics, cross-industry research, behavioral science) in connection with the design, implementation, and modification of DEPs from the perspective of firms, retail investors, and other interested parties? How do these benefits differ depending upon the type of tools or methods? Do the tools and methods mitigate, or have the potential to mitigate, biases in the market that may have prevented participation by some retail investors (e.g., by lowering barriers to entry)? Please provide or identify any relevant data and other information.

2.13 What are the risks and costs associated with the use of the tools and methods identified above (e.g., AI/ML, predictive data analytics, cross-industry research, behavioral science) in connection with the design, implementation, and modification of DEPs from the perspective of firms, retail investors, and other interested parties? How do these risks differ depending upon the type of tools or methods used? What are the most significant investor protection concerns arising from or associated with the use of such tools and methods by broker-dealers and investment advisers in the context of DEPs? Please provide or identify any relevant data and other information.

2.14 What are the similarities and differences between the use of the types of tools and methods identified above in the context of DEPs versus other contexts? Do

commenters believe that certain types of tools or methods are more, less, or as appropriate in the investing context than in other contexts? Please provide or identify any relevant data and other information.

2.15 Are there any particular challenges or risks associated with the use of AI/ML (including deep learning, supervised learning, unsupervised learning, and reinforcement learning), including AI developed or provided by third parties? If so, what are they and how should firms address such challenges or impediments and any risks associated with them? What model risk management steps should firms undertake? Does the use of AI/ML or retail investor data gathered in connection with DEPs raise unique issues related to financial privacy, information security, or identity theft prevention?

2.16 Have researchers (including in the fields of behavioral finance, economics, psychology, marketing, and other related fields) studied the use of such tools and methods in the context of the use of DEPs by firms, or in related contexts of individual decision-making? Please identify any relevant literature or data, including research related to the use of similar practices in other fields, that could assist the Commission in its consideration of these issues.

2.17 To what extent can the use of the tools and methods identified above (e.g., AI/ML models) in connection with the use of DEPs perpetuate social biases and disparities? How, if at all, have commenters seen this in practice with regard to the development and use of DEPs on digital platforms (e.g., through marketing, asset allocation, fees)? Are there AI/ML models that are more or less likely to perpetuate such biases and disparities?

C. REGULATORY ISSUES ASSOCIATED WITH DEPS AND THE RELATED TOOLS AND METHODS AND POTENTIAL APPROACHES

Broker-dealers and investment advisers are currently subject to extensive obligations under federal securities laws and regulations, and in the case of broker-dealers, rules of SROs (in particular, the Financial Industry Regulatory Authority, Inc. ("FINRA")[16]) that are designed to promote conduct that, among other things, protects investors from abusive practices. Following is an overview of some of the existing statutory provisions, regulations, and rules that are particularly relevant to the use of DEPs and related tools and methods by broker-dealers and investment advisers.[17]

In addition to these specific obligations, federal securities laws and regulations broadly prohibit fraud by broker-dealers and investment advisers as well as fraud by any person in the offer, purchase, or sale of securities, or in connection with the purchase or sale of securities. Generally, these anti-fraud provisions cover manipulative or deceptive conduct, including an

---

16 Any person operating as a "broker" or "dealer" in the U.S. securities markets must register with the Commission, absent an exception or exemption. See Exchange Act section 15(a), 15 U.S.C. 78o(a); see also Exchange Act sections 3(a)(4) and 3(a)(5), 15 U.S.C. 78c(a)(4) and 78c(a)(5) (providing the definitions of "broker" and "dealer," respectively). Generally, all registered broker-dealers that deal with the public must become members of FINRA, a registered national securities association, and may choose to become exchange members. See Exchange Act section 15(b)(8), 15 U.S.C. 78o(b)(8); 17 CFR 240.15b9-1. FINRA is the sole national securities association registered with the SEC under Section 15A of the Exchange Act. Because this Request is focused on broker-dealers that deal with the public and are FINRA member firms, we refer to FINRA rules as broadly applying to "broker-dealers," rather than to "FINRA member firms."

17 Broker-dealers and investment advisers are subject to a host of other obligations that are not summarized in this overview, and that may also be relevant to the use of DEPs and related tools and methods. For example, additional regulatory obligations on broker-dealers include those relating to: registration; certain prohibited or restricted conflicts of interest; fair prices, commissions and charges; and best execution. As another example, additional regulatory obligations on investment advisers include those relating to registration; certain prohibited transactions; and written codes of ethics.

affirmative misstatement or the omission of a material fact that a reasonable investor would view as significantly altering the total mix of information made available.[18]

1. Existing Broker-Dealer Obligations:[19]

Under the anti-fraud provisions of the federal securities laws and SRO rules, broker-dealers are required to deal fairly with their customers and observe high standards of commercial honor and just and equitable principles of trade.[20] A number of more specific obligations are summarized below:

- Account Opening and Other Approval Obligations. Broker-dealers must obtain certain information about their customers at account opening, under anti-money laundering

---

18 See Securities Act section 17(a), 15 U.S.C. 77q(a); Exchange Act section 10(b), 15 U.S.C. 78j(b); Exchange Act section 15(c), 15 U.S.C. 78o(c); Investment Advisers Act of 1940 ("Advisers Act") section 206, 15 U.S.C. 80b-6; see also Exchange Act section 9(a), 15 U.S.C. 78i(a); see also Basic v. Levinson, 485 U.S. 224, 239 n.17 (1988).

19 These obligations cannot be waived or contracted away by customers. See Exchange Act section 29(a), 15 U.S.C. 78cc(a) ("Any condition, stipulation, or provision binding any person to waive compliance with any provision of [the Exchange Act] or any rule or regulation thereunder, or any rule of a [SRO], shall be void.").

20 See, e.g., Duker & Duker, Exchange Act Release No. 2350, 6 S.E.C. 386, 388 (Dec. 19, 1939) (Commission opinion) ("Inherent in the relationship between a dealer and his customer is the vital representation that the customer be dealt with fairly, and in accordance with the standards of the profession."); see also U.S. Securities and Exchange Commission, Report of the Special Study of Securities Markets of the Securities and Exchange Commission, H.R. Doc. No. 95, at 238 (1st Sess. 1963) ("An obligation of fair dealing, based upon the general antifraud provisions of the Federal securities laws, rests upon the theory that even a dealer at arm's length impliedly represents when he hangs out his shingle that he will deal fairly with the public."); FINRA Rule 2010 (Standards of Commercial Honor and Principles of Trade); NASD Interpretive Material 2310-2 (Fair Dealing with Customers) ("Implicit in all member and registered representative relationships with customers and others is the fundamental responsibility for fair dealing. Sales efforts must therefore be undertaken only on a basis that can be judged as being within the ethical standards of [FINRA's] Rules, with particular emphasis on the requirement to deal fairly with the public.").

("AML") and know your customer requirements,[21] and are required to maintain customer account information, including whether a customer is of legal age.[22]

Additional obligations apply for investors to transact in certain types of securities (e.g., options) or obtain certain services (e.g., margin).[23] For example, broker-dealers

---

21 Financial institutions, including broker-dealers, are required to establish written customer identification programs (CIP), which must include, at a minimum, procedures for: obtaining customer identifying information from each customer prior to account opening; verifying the identity of each customer, to the extent reasonable and practicable, within a reasonable time before or after account opening; making and maintaining a record of information obtained relating to identity verification; determining within a reasonable time after account opening or earlier whether a customer appears on any list of known or suspected terrorist organizations designated by Treasury; and providing each customer with adequate notice, prior to opening an account, that information is being requested to verify the customer's identity. See 31 CFR 1023.220 (Customer Identification Program for Broker-Dealers). As part of broker-dealers' AML compliance programs, they must include risk-based procedures for conducting ongoing customer due diligence, to comply with the Customer Due Diligence Requirements for Financial Institutions ("CDD Rule") of the Financial Crimes Enforcement Network (FinCEN). See FINRA Rule 3310 (Anti-Money Laundering Compliance Program); 81 FR 29398 (May 11, 2016) (CDD Rule Release); 82 FR 45182 (Sept. 28, 2017) (correction to CDD Rule amendments). Additionally, pursuant to FINRA Rule 2090 (Know Your Customer), all member broker-dealers must use reasonable diligence, at both the opening of a customer account, and for the duration of the customer relationship to know and retain the "essential facts" concerning each customer. Such "essential facts" include those that are necessary "to (a) effectively service the customer's account, (b) act in accordance with any special handling instructions for the account, (c) understand the authority of each person acting on behalf of the customer, and (d) comply with applicable laws, regulations, and rules." See FINRA Regulatory Notice 11-02 (SEC Approves Consolidated FINRA Rules Governing Know-Your-Customer and Suitability Obligations); see also 17 CFR 240.17a-3(a)(17).

22 See FINRA Rule 4512 (Customer Account Information). As a general matter, whether any particular individual is able to enter into a contract (such as that associated with opening a brokerage account) is a matter of state law, and not explicitly governed by the federal securities laws. See also 17 CFR 240.17a-3(a)(17).

23 Approval obligations also apply for investors to engage in day-trading. See FINRA Rule 2130 (Approval Procedures for Day-Trading Accounts).

must pre-approve a customer's account to trade options on securities.[24] Prior to approving a customer's account for options trading, the broker-dealer must seek to obtain "essential facts relative to the customer, [their] financial situation and investment objectives."[25] Broker-dealers must then verify the background and financial information they obtain regarding each customer, and obtain an executed written agreement from the customer agreeing, among other things, to be bound by all applicable FINRA rules applicable to the trading of option contracts.[26]

With respect to margin, broker-dealers are required to obtain the signature of the account owner with respect to a margin account[27] and to obtain a customer's written

---

24 See FINRA Rule 2360(b)(16) (Options). FINRA has also extended the options account approval requirements of Rule 2360(b)(16), by reference, to customers seeking to place orders to buy or sell warrants. See FINRA Rule 2352 (Account Approval). Numerous exchanges that facilitate options trading apply similar standards for customer pre-approval before accepting orders for options contracts on the exchange.

25 See FINRA Rule 2360(b)(16)(B).

26 See FINRA Rule 2360(b)(16)(C) and (D). FINRA has also indicated that in the case of options, broker-dealers should consider whether they should provide limited account approval to a customer, based on this information. For example, customers may be approved to make purchases of puts and calls only, be restricted to covered call writing, or be approved to engage in uncovered put and call writing. See FINRA Regulatory Notice 21-15 (FINRA Reminds Members About Options Account Approval, Supervision and Margin Requirements).

27 See 17 CFR 240.17a-3(a)(9).

consent.[28] These written consents and signatures are generally obtained by broker-dealers when a customer executes a margin agreement.[29]

- Standard of Conduct. Regulation Best Interest ("Reg BI") requires broker-dealers that make recommendations of securities transactions or investment strategies involving securities (including account recommendations) to retail customers to act in their best interest, and not place the broker-dealer's interests ahead of the retail customer's interest.[30] The use of a DEP by a broker-dealer may, depending on the relevant facts and circumstances, constitute a recommendation for purposes of Reg BI. Whether a "recommendation" has been made is interpreted consistent with precedent under the federal securities laws and how the term has been applied under FINRA rules.[31] Broker-

---

28 The written consent is a condition necessary for the broker-dealer to be able to hypothecate (i.e., pledge) securities under circumstances that would permit the commingling of customers' securities. Broker-dealers are also required to give written notice to a pledgee that, among other things, a security pledged is carried for the account of a customer. See 17 CFR 240.8c-1 and 240.15c2-1.

29 See 17 CFR 240.8c-1, 240.15c2-1, and 240.17a-3(a)(9). Margin agreements also typically state that a customer must abide by the margin requirements established by the Federal Reserve Board, SROs such as FINRA, any applicable securities exchange, and the firm where the margin account is established. See also FINRA Rule 4210(f)(8)(B) (Margin Requirements) regarding special margin requirements for day trading, including special requirements for "pattern day traders" (any customer who executes four or more day trades within five business days, provided that the number of day trades represents more than six percent of the customer's total trades in the margin account for that same five business day period).

30 17 CFR 240.15l-1; Regulation Best Interest: The Broker-Dealer Standard of Conduct, Exchange Act Release No. 34-86031 [84 FR 33318 (July 12, 2019)] ("Reg BI Adopting Release"). Following the adoption of Reg BI, which, among other things, incorporated and enhanced the principles found in FINRA's suitability rule (Rule 2111), FINRA amended Rule 2111 to, among other things, state that the rule does not apply to recommendations subject to Reg BI. See Exchange Act Release No. 89091 (June 18, 2020) [85 FR 37970 (June 24, 2020)].

31 Reg BI Adopting Release, supra note 30, at 33337. The determination of whether a recommendation has been made turns on the facts and circumstances of a particular

dealers satisfy their obligations under Reg BI by complying with four specified component obligations: a disclosure obligation;[32] a care obligation;[33] a conflict of interest obligation;[34] and a compliance obligation.[35] Additional suitability obligations are imposed on broker-dealers when recommending transactions in certain types of securities, such as options, to any customer.[36]

---

situation. Id. at 33335 ("Factors considered in determining whether a recommendation has taken place include whether a communication 'reasonably could be viewed as a "call to action"' and 'reasonably would influence an investor to trade a particular security or group of securities.' The more individually tailored the communication to a specific customer or a targeted group of customers about a security or group of securities, the greater the likelihood that the communication may be viewed as a 'recommendation.'") (citation omitted); see also NASD Notice to Members 01-23 (Apr. 2001) (Online Suitability—Suitability Rules and Online Communications) (providing examples of electronic communications that are considered to be either within or outside the definition of "recommendation"). To the extent that a broker-dealer makes a recommendation, as that term is interpreted by the Commission under Reg BI, to a retail customer through or in connection with a DEP, Reg BI would apply to the recommendation.

32 The disclosure obligation requires the broker-dealer to provide certain required disclosure before or at the time of the recommendation, about the recommendation and the relationship between the broker-dealer and the retail customer. 17 CFR 240.15l-1(a)(2)(i).

33 The care obligation requires the broker-dealer to exercise reasonable diligence, care, and skill in making the recommendation. 17 CFR 240.15l-1(1)(a)(2)(ii).

34 The conflict of interest obligation requires the broker-dealer to establish, maintain, and enforce written policies and procedures reasonably designed to address conflicts of interest associated with its recommendations to retail customers. Among other specific requirements, broker-dealers must identify and disclose any material limitations, such as a limited product menu or offering only proprietary products, placed on the securities or investment strategies involving securities that may be recommended to a retail customer and any conflicts of interest associated with such limitations, and prevent such limitations and associated conflicts of interest from causing the broker-dealer or the associated person to place the interest of the broker-dealer or the associated person ahead of the retail customer's interest. 17 CFR 240.15l-1(a)(2)(iii).

35 The compliance obligation requires the broker-dealer to establish, maintain, and enforce written policies and procedures reasonably designed to achieve compliance with Reg BI. 17 CFR 240.15l-1(a)(2)(iv).

36 See, e.g., FINRA Rule 2360(b)(19).

- Disclosure Obligations. Broker-dealers are subject to a number of customer disclosure obligations, including disclosures at the inception of the customer relationship,[37] disclosures that must be made in conjunction with recommendations of securities transactions or investment strategies involving securities,[38] and certain product- or activity-specific disclosures pertaining to among others, options, margin, and day trading.[39] Additionally, broker-dealers are liable under the anti-fraud provisions for failing to disclose material information to their customers when they have a duty to make such disclosure.[40] Broker-dealers are also required to make disclosures to customers of their order execution and routing practices.[41]

---

37 Disclosure obligations include Form CRS relationship summary (describing the broker-dealer's services, fees, costs, conflicts of interest and disciplinary history). See 17 CFR 240.17a-14.

38 See 17 CFR 240.15l-1 (Reg BI).

39 See, e.g., FINRA Rule 2360(b)(16)(A) (requiring broker-dealers to provide certain risk disclosures when approving customers for options transactions); FINRA Rule 2264 (Margin Disclosure Statement) (specifying disclosures in advance of opening a margin account for a non-institutional customer); 17 CFR 240.10b-16 (requiring disclosures of all credit terms in connection with any margin transactions at account opening); FINRA Rule 2270 (Day-Trading Risk Disclosure Statement) (requiring that a disclosure statement be provided to any non-institutional customer that opens an account at a broker-dealer that promotes a day-trading strategy).

40 See Basic v. Levinson, supra note 18. Generally, under the anti-fraud provisions, a broker-dealer's duty to disclose material information to its customer is based upon the scope of the relationship with the customer, which depends on the relevant facts and circumstances. See, e.g., Conway v. Icahn & Co., Inc., 16 F.3d 504, 510 (2d Cir. 1994) ("A broker, as agent, has a duty to use reasonable efforts to give its principal information relevant to the affairs that have been entrusted to it.").

41 See generally 17 CFR 242.605 and 242.606 (Regulation NMS Rules 605 and 606). For example, under NMS Rule 606, broker-dealers must provide public reports concerning the venues to which they route customer orders for execution and discuss material aspects of their arrangements with these execution venues, including PFOF that broker-dealers receive from the venues. Pursuant to amendments implemented in 2020, these reports require enhanced specificity concerning PFOF and other types of practices that may

- Reporting and Other Financial Responsibility Requirements. Broker-dealers are subject to comprehensive financial responsibility rules, including reporting requirements under Exchange Act Rule 17a-5, minimum net capital requirements under Exchange Act Rule 15c3-1, and customer protection requirements under Exchange Act Rule 15c3-3.[42] Broker-dealers are also subject to various rules relating to margin, including, for example, disclosure and other requirements when extending or arranging credit in certain transactions,[43] disclosure of credit terms in margin transactions,[44] a description of the margin requirements that determine the amount of collateral customers are expected to

present broker-dealer conflicts of interest. See Exchange Act Release No. 78309 (Nov. 2, 2018) [83 FR 58338, 58373-6 (Nov. 19, 2018)].

42 Rule 17a-5 has two main elements: (1) a requirement that broker-dealers file periodic unaudited reports about their financial and operational condition using the FOCUS Report form; and (2) a requirement that broker-dealers annually file financial statements and certain reports, as well as reports covering those statements and reports prepared by an independent public accountant registered with the Public Company Accounting Oversight Board ("PCAOB") in accordance with PCAOB standards. 17 CFR 240.17a-5. The objective of Rule 15c3-1 is to require a broker-dealer to maintain sufficient liquid assets to meet all liabilities, including obligations to customers, counterparties, and other creditors and to have adequate additional resources to wind-down its business in an orderly manner without the need for a formal proceeding if the firm fails financially. See 17 CFR 240.15c3-1. Rule 15c3-3 requires a carrying broker-dealer to maintain physical possession or control over customers' fully paid and excess margin securities. The rule also requires a carrying broker-dealer to maintain a reserve of funds or qualified securities in an account at a bank that is at least equal in value to the net cash owed to customers. 17 CFR 240.15c3-3.

43 See 17 CFR 240.15c2-5 (Disclosure and other requirements when extending or arranging credit in certain transactions).

44 See 17 CFR 240.10b-16 (Disclosure of credit terms in margin transactions).

maintain in their margin accounts,[45] and a requirement to issue a margin disclosure statement prior to opening a margin account.[46]

- Communications with the Public Rules. Broker-dealers are subject to a number of rules governing communications with the public, including advertising or marketing communications. These rules apply to broker-dealers' written (including electronic) communications with the public and are subject to obligations pertaining to content, supervision, filing, and recordkeeping.[47] All communications must be based on principles of fair dealing and good faith, be fair and balanced, and comply with a number

---

45 See FINRA Rule 4210 (Margin Requirements). See also 12 CFR 220.1 et seq. (Federal Reserve Board's Regulation T regulating, among other things, extensions of credit by brokers and dealers);

46 See FINRA Rule 2264 (Margin Disclosure Statement). See also FINRA Regulatory Notice 21-15 (FINRA Reminds Members About Options Account Approval, Supervision and Margin Requirements).

47 See, e.g., FINRA Rule 2210 (Communications with the Public). FINRA has provided guidance regarding the applicability of the communications rules in the context of social media and digital communications. See FINRA Regulatory Notice 19-31 (Disclosure Innovations in Advertising and Other Communications with the Public); FINRA Regulatory Notice 17-18 (Social Media and Digital Communications); FINRA Regulatory Notice 11-39 (Social Media Websites and the Use of Personal Devices for Business Communications); FINRA Regulatory Notice 10-06 (Social Media Web Sites); see also 17 CFR 240.17a-4(b)(4). Paragraph (b)(4) of Rule 17a-4 requires a broker-dealer to preserve originals of all communications received and copies of all communications sent (and any approvals thereof) by the broker-dealer (including inter-office memoranda and communications) relating to its business as such, including all communications which are subject to the rules of an SRO of which the broker-dealer is a member regarding communications with the public. The term "communications," as used in paragraph (b)(4) of Rule 17a-4, includes all electronic communications (e.g., emails and instant messages). See Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security-Based Swap Participants, and Broker-Dealers, Exchange Act Release No. 87005 (Sept. 19, 2019) [84 FR 68550, 68563-64 (Dec. 16, 2019)].

of other content standards.[48] Through its filings review program, FINRA's Advertising Regulation Department reviews communications submitted either voluntarily or as required by FINRA rules.[49] In the case of communications relating to options, broker-dealers are subject to certain heightened obligations.[50]

- Supervision Obligations and Insider Trading Procedures. Broker-dealers must "establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules."[51] Among other things, broker-dealers must establish, maintain, and enforce written procedures to supervise the types of business in which they engage and the activities of their associated persons that are reasonably designed to achieve compliance with applicable securities laws and

---

48 Among other requirements and prohibitions, firms may not "make any false, exaggerated, unwarranted, promissory or misleading statement or claim in any communication;" firms "must ensure that statements are clear and not misleading within the context in which they are made, and that they provide balanced treatment of risks and potential benefits;" and firms "must consider the nature of the audience to which the communication will be directed and must provide details and explanations appropriate to the audience." See FINRA Rule 2210 (Communications with the Public).

49 FINRA reviews communications for compliance with applicable regulations. Broker-dealers must submit certain retail communications to FINRA for its approval at least ten business days prior to first use or publication. In addition to reviewing filed communications, broker-dealer communications can also be subject to spot-check reviews by FINRA. See FINRA Rule 2210(c).

50 See FINRA Rule 2220 (Options Communications). For example, when making retail communications concerning the sale of options products, broker-dealers must submit certain of those communications to FINRA for its approval at least ten calendar days prior to use.

51 See FINRA Rule 3110 (Supervision). Under Exchange Act Sections 15(b)(4)(E) and 15(b)(6), the Commission institutes administrative proceedings against broker-dealers and supervisors for failing reasonably to supervise, with a view to preventing violations of the federal securities laws. 15 U.S.C. 78o(b)(4)(E) and 78o(b)(6).

regulations, and with applicable FINRA rules.[52] Broker-dealers must also establish, maintain, and enforce written policies and procedures reasonably designed to prevent the misuse of material, nonpublic information by the broker-dealer or its associated persons.[53]

- Recordkeeping Obligations. Section 17(a) of the Exchange Act provides the Commission with authority to issue rules requiring broker-dealers to make and keep for prescribed periods such records as the Commission, by rule, prescribes as necessary or appropriate in the public interest, for the protection of investors, or otherwise in furtherance of the purposes of the Exchange Act. Rules 17a-3 and 17a-4 prescribe the primary recordkeeping requirements for broker-dealers.[54]
- Customer Complaints. Broker-dealers are required to have procedures to document and capture, acknowledge, and respond to all written (including electronic) customer complaints,[55] and report to FINRA certain specified events related to customer complaints, as well as statistical and summary information on customer complaints.[56]

---

52 See FINRA Rule 3110(b)(1).

53 See Exchange Act section 15(g), 15 U.S.C. 78o(g).

54 Exchange Act Rule 17a-3 (delineating certain records that broker-dealers must make and keep current, including customer account records, copies of customer confirmations, records of customer complaints, and records related to every recommendation of any securities transaction or investment strategy involving securities made to a retail customer); Exchange Act Rule 17a-4 (specifying the time period and manner in which records made pursuant to Rule 17a-3 must be preserved, and identifying additional records that must be maintained for prescribed time periods.). See 17 CFR 240.17a-3 and 240.17a-4.

55 See FINRA Rule 3110(b)(5).

56 See FINRA Rule 4530; see also FINRA Rule 4311(g) (addressing certain requirements for carrying agreements relating to customer complaints).

Broker-dealers must also make and keep a record indicating that each customer has been provided with a notice with the address and telephone number to which complaints may be directed.[57]

- Privacy and Cybersecurity. Regulation S-P requires broker-dealers to disclose certain information about their privacy policies and practices, limits the instances in which broker-dealers may disclose nonpublic personal information about consumers to nonaffiliated third parties without first allowing the consumer to opt out, and requires broker-dealers to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.[58] Regulation S-P also limits the re-disclosure and re-use of nonpublic personal information, and it limits the sharing of account number information with nonaffiliated third parties for use in telemarketing, direct mail marketing, and email marketing.[59] Broker-dealers are also required, under Regulation S-ID, to develop and implement a written identity theft prevention program designed to detect, prevent, and

---

57 See 17 CFR 240.17a-3(a)(18) (requiring broker-dealers to make and maintain a record for each written customer complaint received regarding an associated person, including the disposition of the complaint).

58 See 17 CFR 248. Regulation S-P implements the consumer financial privacy provisions, as well as the customer records and information security provisions, of Title V of the Gramm Leach Bliley Act ("GLBA"). It also implements the consumer report information disposal provisions (Section 628) of the Fair Credit Reporting Act ("FCRA") as amended by the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act").

59 See 17 CFR 248.11 and 248.12.

mitigate identity theft in connection with certain existing accounts or the opening of new accounts.[60]

2. Existing Investment Adviser Obligations:

The Investment Advisers Act of 1940 ("Advisers Act") establishes a federal fiduciary duty for investment advisers, whether or not registered with the Commission, which is made enforceable by the anti-fraud provisions of the Advisers Act. The fiduciary duty is broad and applies to the entire adviser-client relationship, and must be viewed in the context of the agreed-upon scope of that relationship.[61] As a fiduciary, an investment adviser owes its clients a duty of care and a duty of loyalty.[62] Under its duty of loyalty, an adviser must make full and fair disclosure of all material facts relating to the advisory relationship and must eliminate or make full and fair disclosure of all conflicts of interest which might incline an investment adviser—consciously or unconsciously—to render advice which is not disinterested such that a client can provide informed consent to the conflict. An adviser's duty of care includes, among other things: (i) a duty to provide investment advice that is in the best interest of the client, based on a

---

60 See 17 CFR 248.201. Regulation S-ID implements the identity theft red flags rules and guidelines provisions (Section 615(e)) of the FCRA as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("Dodd-Frank Act").

61 For example, to the extent that an adviser provides investment advice to a client through or in connection with a DEP, then all such investment advice must be consistent with the adviser's fiduciary duty.

62 This fiduciary duty "requires an adviser to adopt the principal's goals, objectives, or ends." See Commission Interpretation Regarding Standard of Conduct for Investment Advisers, Advisers Act Release No. 5248 (June 5, 2019) [84 FR 33669, 33671 (July 12, 2019)] ("IA Fiduciary Duty Interpretation") (internal quotations omitted). This means the adviser must, at all times, serve the best interest of its client and not subordinate its client's interest to its own. See id.

reasonable understanding of the client's objectives;[63] (ii) a duty to seek best execution of a client's transactions where the adviser has the responsibility to select broker-dealers to execute client trades (typically in the case of discretionary accounts); and (iii) a duty to provide advice and monitoring at a frequency that is in the best interest of the client, taking into account the scope of the agreed relationship.[64] We discussed the fiduciary duty and these aspects of it in greater detail in a Commission interpretation.[65]

Rules adopted under the Advisers Act also impose various obligations on registered investment advisers (or investment advisers required to be registered with the Commission), including:

- Disclosure Requirements. Registered investment advisers are subject to a number of client disclosure obligations, including disclosures before or at the time of entering into an advisory contract, annually thereafter, and when certain changes occur. These disclosures include information about a number of topics, including an adviser's business practices, fees, conflicts of interest, and disciplinary information, and about advisory employees and their other business activities.[66]
- Reporting Requirements. Investment advisers register with the Commission by filing Form ADV and are required to file periodic updates.[67] Like all market participants,

---

63 In order to provide such advice, an investment adviser must have a reasonable understanding of the client's objectives. See id. at 33672-3.

64 See id. at 33669-78.

65 See id.

66 See, e.g., 17 CFR 275.204-3 (requiring an adviser to deliver a Form ADV Part 2A brochure to advisory clients); 17 CFR 275.204-5 (requiring an adviser to deliver Form CRS to each retail investor).

67 See, e.g., 17 CFR 275.204-1.

investment advisers are subject to reporting obligations under the Exchange Act under specified circumstances,[68] as well as trading rules and restrictions under the Exchange Act.[69]

- Marketing Requirements. Rule 206(4)-1, as amended in December 2020, governs investment advisers' marketing practices.[70] This rule contains seven general prohibitions on the types of activity that could be false or misleading that apply to all advertisements. The rule also prohibits advertisements that contain testimonials, endorsements, third-party ratings, and performance information, unless certain conditions are met.
- Compliance Programs. Under rule 206(4)-7, an investment adviser must adopt and implement written policies and procedures reasonably designed to prevent violation of the Advisers Act and the rules thereunder by the firm and its supervised persons.[71] Among other things, an adviser's compliance policies and procedures should address portfolio management processes, including allocation of investment opportunities among clients and consistency of portfolios with clients' investment objectives, disclosures by the adviser, and applicable regulatory restrictions. This rule requires review of such

---

68 These include, for example, Schedule 13D or Schedule 13G reporting of "beneficial ownership" of more than 5 percent of shares of a voting class of a security registered under Section 12 of the Exchange Act and Form 13F quarterly reports filed by institutional investment managers that manage more than $100 million of specified securities. See 17 CFR 240.13d-1(a)-(c) and 240.13f-1.

69 These include prohibitions and restrictions on market manipulation and insider trading. See, e.g., 17 CFR 240.10b5-1 and 240.10b5-2.

70 The compliance date for amended rule 206(4)-1 under the Advisers Act is November 4, 2022. Until then, advisers that do not comply with amended 206(4)-1 must comply with existing rule 206(4)-1, which governs adviser's advertisements, and rule 206(4)-3, which governs cash payments for client solicitations.

71 See 17 CFR 275.206(4)-7.

policies and procedures at least annually, and the designation of a chief compliance officer responsible for administering such policies and procedures.

- Supervision Obligations and Insider Trading Procedures. Investment advisers have a duty to reasonably supervise certain persons with respect to activities performed on the adviser's behalf.[72] In addition, section 204A of the Advisers Act requires investment advisers (registered with the Commission or not) to establish, maintain, and enforce written policies and procedures reasonably designed to prevent the misuse of material, nonpublic information by the investment adviser or any of its associated persons.
- Recordkeeping Requirements. Under rule 204-2, investment advisers must make and keep particular books and records, including certain communications relating to advice given (or proposed to be given), the placing or execution of any order to purchase or sell any security, and copies of the advertisements they disseminate.[73]
- Privacy and Cybersecurity. Advisers registered or required to be registered with the Commission are also subject to Regulation S-P and Regulation S-ID, which are discussed above in the context of broker-dealers.

Questions: Current regulatory compliance approaches:

3.1 How are firms approaching compliance relating to their use of DEPs and the related tools and methods, in order to ensure compliance with their obligations under federal securities laws and regulations, including those identified above? For example, how do firms supervise communications or marketing to retail investors through or in connection with DEPs? Do firms approach compliance relating to the use of DEPs

72 See Advisers Act section 203(e)(6), 15 U.S.C. 80b-3(e)(6).

73 See 17 CFR 275.204-2.

and related tools and methods differently from how they approach compliance relating to other engagement with customers or clients? If so, how do the approaches differ? For example, do such approaches differ based on any unique risks associated with or innate characteristics of DEPs and the related tools and methods?

3.2 What types of policies and procedures and controls do firms establish and maintain to ensure the design, development, and use of DEPs and related tools and methods comply with existing obligations? How do firms supervise the design, development, and use of these features, tools, and methods after implementation and adoption for continued compliance? In what ways do firms' policies and procedures, controls, and supervision differ with respect to their use of DEPs and related tools and methods from other policies and procedures, controls, and supervision that the firms employ?

3.3 Do firms implement registration or certification requirements for personnel primarily responsible for the design, development, and supervision of DEPs? If so, what are the requirements? What type of training do firms offer to their personnel in connection with the design, development, and use of DEPs and related tools and methods? Do firms outsource the design or development of DEPs? Do firms outsource the design and development of DEPs outside the United States?

3.4 What policies, procedures, and controls do firms have in place with respect to the use of DEPs that are designed to promote or that could otherwise direct retail investors to higher-risk products and services, for example, margin services and options trading? What policies, procedures, and controls do firms have in place with respect to the use of DEPs that are designed to promote or that could otherwise direct retail investors to securities or services that are more lucrative for the firm such as: proprietary

products, products for which the firm receives revenue sharing or other third-party payments, or other higher fee products? To what extent do these policies and procedures consider or address the characteristics of retail investors to whom such products and services may be promoted or directed? For example, do the policies and procedures place controls around how DEPs may be utilized to promote or otherwise direct certain products or services to certain types of retail investors?

3.5 What disclosures are firms providing in connection with or specifically addressing DEPs and the related tools and methods (including with respect to any data or information collected from the retail investor)? How are such disclosures presented to retail investors? Does such disclosure address how the use of DEPs or the related tools and methods may affect investors and specifically their trading and investing behavior? Does such disclosure differ from other disclosures that firms provide? How do firms currently disclose information such as risks, fees, costs, conflicts of interest, and standard of conduct to retail investors on their digital platforms? To what extent and how do firms use DEPs to make such disclosures?

3.6 Do broker-dealers consider the observable impacts of DEPs when determining if they are making "recommendations" for purposes of Reg BI? How does the fact that a DEP might impact the behavior of a statistically significant number of retail investors affect this determination? What statistical concepts, tools, and quantitative thresholds do broker-dealers use in making this determination?

3.7 Are there particular types of DEPs that broker-dealers avoid using because they would be recommendations? If so, which DEPs and why? What are broker-dealers

doing to ensure that the DEPs they adopt comply with Reg BI and other sales practice rules, where applicable?

3.8 Do investment advisers consider the observable impacts of DEPs when determining if they are providing investment advice? How does the fact that a DEP might impact the behavior of a statistically significant number of investors affect this determination? What statistical concepts, tools, and quantitative thresholds do investment advisers use in making this determination?

3.9 Are there particular types of DEPs that investment advisers avoid using because they would constitute providing investment advice? If so, which DEPs and why? How do investment advisers satisfy their fiduciary duty when using DEPs and related tools and methods? How do investment advisers take into account their fiduciary duty when designing and developing DEPs?

3.10 When providing investment advice or recommendations to a retail investor, do firms adjust that investment advice or recommendation to take into account any data they have about how their DEPs affect investor behavior and investing outcomes? If so, how is such investment advice or recommendation adjusted?

3.11 How do firms using DEPs obtain sufficient retail investor information and provide sufficient oversight to satisfy their regulatory obligations, including, for example, applicable anti-fraud provisions and account opening or approval requirements?

3.12 How does the recordkeeping process used by firms in connection with DEPs and the related tools and methods compare to the recordkeeping process used in connection with firms' traditional business? Do firms generate and retain records with respect to the development, implementation, modification, and use of DEPs, including the

testing of, or due diligence with respect to, the technology that they use for those purposes? Do firms generate and retain records with respect to retail investor interaction with such DEPs? If so, what types of records?

Questions: Suggestions for modifications to existing regulations or new regulatory approaches to address investor protection concerns, including:

3.13 What additions or modifications to existing regulations, including, but not limited to, those identified above, or new regulations or guidance might be warranted to address investor protection concerns identified in connection with the use by broker-dealers and investment advisers of DEPs, the related tools and methods, and the use of retail investor data gathered in connection with DEPs? What types of requirements, limitations, or prohibitions would be most appropriate to address any such identified investor protection concerns?

3.14 Are there regulations that currently prevent firms from using DEPs and related tools and methods in ways that might be beneficial to retail investors? If so, what additions or modifications to those regulations would make it easier for firms to use DEPs and related tools and methods to benefit investors? Are there regulatory approaches that would facilitate firms' ability to innovate or test the use of new technology consistent with investor protection?

3.15 To the extent commenters recommend any modifications to existing regulations or new regulations, how should DEPs and the scope of tools and methods be defined to capture practices and tools and methods in use today and remain flexible to adapt as technology changes? Should any such modifications or new regulations specifically and uniquely address DEPs or the related tools and methods (i.e., distinct from regulation of interactions with retail investors such as marketing, investment advice,

and recommendations)? If so, how? Should any such modifications or additional regulations be targeted specifically to address certain types of DEPs or certain tools or methods? If so, how? For example, should specific DEPs be explicitly prohibited or only permitted subject to limitations or other regulatory requirements (e.g., filing or pre-approval)?

3.16 Should any such modifications or additional regulations be targeted specifically to address particular risks, such as those related to certain types of securities (e.g., options, leveraged and inverse funds, or other complex securities), services (e.g., margin), or conflicts (e.g., payment and revenue sources)? If so, how? Should any such modifications or additional regulations be targeted specifically to increase protection for certain categories of investors (e.g., seniors or inexperienced investors)? If so, how?

3.17 Are there laws, regulations, or other conduct standards that have been adopted in other contexts, fields, or jurisdictions that could serve as a useful model for any potential regulatory approaches?

3.18 To the extent commenters recommend any modifications to existing regulations or new regulations, what economic costs and benefits do commenters believe would result from their recommendations? Please provide or identify any relevant data and other information.

III. USE OF TECHNOLOGY BY INVESTMENT ADVISERS TO DEVELOP AND PROVIDE INVESTMENT ADVICE

The Commission is also issuing the Request to assist the Commission and its staff in better understanding the nature of analytical tools and other technology used by investment advisers to develop and provide investment advice to clients, including (1) oversight of this

technology; (2) how investment advisers and clients have benefited from technology; (3) potential risks to investment advisers, clients, and the markets more generally related to this technology; and (4) whether regulatory action may be needed to protect investors while preserving the ability of investors to benefit from investment advisers' use of technology.[74]

A. ISSUES FOR CONSIDERATION

Financial technology enables investment advisers to develop and provide investment advice in new ways or complements existing methods or tools for developing and providing advice,[75] including by allowing digital platforms to connect clients, their investment advisers, and third-party service providers.[76] We describe below some recent changes in delivery and development of investment advice and the role of analytical tools and other technology in each. These changes are those that we understand may directly affect clients' receipt of investment advice, and some may overlap depending on an adviser's particular business model and services.

While the increased role of technology has presented investment advisers and clients with benefits, it may also present risks. We recognize that some of these risks may be presented, or be presented differently, for advisers providing traditional investment advice that does not rely

---

74 While we recognize that broker-dealers similarly use analytical tools and other technology for purposes of developing and providing recommendations, those issues are not the focus of Section III of the Request. However, the Commission welcomes comments on these issues relating to broker-dealers as part of the General Request for Comment as set forth in Section IV below.

75 The International Organization of Securities Commissions ("IOSCO") has stated that the terms financial technologies or "Fintech" are "used to describe a variety of innovative business models and emerging technologies that have the potential to transform the financial services industry." IOSCO Research Report on Financial Technologies (Fintech) at 4 (Feb. 2017), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf.

76 Many investment advisers also increasingly use third-party service providers to generate investment models (e.g., model portfolios) or strategies, and may use software based on, or otherwise incorporating, AI/ML models.

on technology. We understand as well that investment advisers may weigh differently those potential benefits and risks, including those described below, in determining how to use technology in developing and providing investment advice. We therefore are seeking comment to understand better the tools used by investment advisers to develop and provide investment advice and investment advisers' understanding and oversight of these tools and the related benefits and risks. In addition, we seek comment on other ways in which technology has changed investment advisers' development and provision of investment advice to their clients.

1. Robo-Advisers.

Some investment advisers, which we refer to here as robo-advisers, provide asset management services to their clients through online algorithm-based platforms.[77] The number of robo-advisers (also referred to as digital investment advisers, digital advisers, or automated advisers) has increased over the past several years.[78] Robo-advisers operate under a variety of business models and have varying degrees of human interaction with clients as compared to traditional advisers, and some rely exclusively on algorithms to oversee and manage individual

---

77 An algorithm can be defined as a routine process or sequence of instructions for analyzing data, solving problems, and performing tasks. See Dilip Krishna et al., Managing Algorithmic Risks: Safeguarding the Use of Complex Algorithms and Machine Learning at 3, Deloitte Development LLC (2017) ("Deloitte Report").

78 See, e.g., Investment Adviser Association, 2020 Evolution Revolution at 8 (2020), https://higherlogicdownload.s3.amazonaws.com/INVESTMENTADVISER/aa03843e-7981-46b2-aa49-c572f2ddb7e8/UploadedImages/resources/Evolution_Revolution_2020_v8.pdf (noting that by 2020, "two of the top five advisers as measured by number of non-high net worth individual clients served [were] digital advice platforms, representing 7.5 million clients, an increase of 2.7 million clients from [the prior year]."); Robo-Advisers, IM Guidance Update No. 2017-02 (Feb. 2017), https://www.sec.gov/investment/im-guidance-2017-02.pdf.

client accounts.[79] In some cases, human personnel may have limited ability to override an algorithm, even in stressed market conditions, and there is limited, if any, direct interaction between the client and the adviser's personnel. In other cases, robo-advisers offer hybrid advisory services, which pair algorithm-generated investment options with human personnel who can answer questions, discuss and refine an algorithm-generated investment plan (e.g., clarify information where client questionnaire responses seem conflicting or address risk tolerance levels based on client reaction to stressed market conditions), or provide additional resources to clients. Some robo-advisers offer clients a choice between hybrid and non-hybrid services, at different price points.

In addition to using analytical tools to engage with clients, robo-advisers may use technology (including AI/ML tools) for a variety of other functions. For example, an adviser may use these tools to match clients to individual portfolios based on client inputs or determine how or when to trade for individual client accounts. An adviser also may use these tools to determine asset allocations, determine how to fill allocations, generate trading signals, or make other strategic decisions.[80]

---

79 A robo-adviser or a third party may develop, manage, or own the algorithm used to manage client accounts. In some business models, a robo-adviser may provide its algorithm or its digital platform to another investment adviser. That investment adviser may then (i) use the robo-adviser's existing investment options (e.g., asset allocation models), (ii) use the algorithm or digital platform as a tool to create its own investment options, or (iii) use a combination of these features.

80 In addition, FINRA has observed client-facing digital advisers that incorporate trade execution, portfolio rebalancing, and tax-loss harvesting. See FINRA, Report on Digital Investment Advice at 2 (Mar. 2016), https://www.finra.org/sites/default/files/digital-investment-advice-report.pdf (describing digital investment tools as tools within two groups: financial professional-facing tools and client-facing tools).

All Commission-registered robo-advisers are subject to all of the requirements of the Advisers Act, including the requirement that they provide advice consistent with the fiduciary duty they owe to clients.[81] Because robo-advisers rely on algorithms, provide advisory services over the internet, and may offer limited, if any, direct human interaction to their clients, they may raise novel issues when seeking to comply with the Advisers Act. For example, advisers may need to consider whether and how automation affects the development of digital advice and the potential risks that such automation may present. An automated algorithm may produce investment advice for a particular client that is inconsistent with the client's investment strategy or relies on incomplete information about the client that depends on limited input data. Increased reliance on automated investment advice may result in too much importance being placed on clients' responses to account opening questionnaires and other forms of automated client evaluation, which may not permit nuanced answers or determine when additional clarification or information could be necessary. This reliance may also result in a failure to detect changes in clients' circumstances that may warrant a change in investment strategy.

Robo-advisers also must determine how to effectively understand and oversee use of their algorithms (including those developed by third parties) and the construction of client portfolios, including any potential conflicts of interest. For example, robo-advisers' algorithms may result in clients being invested in assets in which the adviser or its affiliate holds interests or advises separately (e.g., mutual funds and exchange-traded funds). In these circumstances, the adviser would have a conflict of interest that it must eliminate or fully and fairly disclose such that the client can provide informed consent. In addition, any override or material changes to the

---

81 See IA Fiduciary Duty Interpretation, supra note 62, at n.27.

algorithm must result in investment advice that is consistent with the adviser's disclosures and fiduciary duty.

2. Internet Investment Advisers.

Some investment advisers may solely use an interactive website to provide investment advice. These investment advisers, otherwise known as "internet investment advisers," are eligible for SEC registration even if they do not meet the assets-under-management threshold if they satisfy certain criteria, including that they provide advice to all of their clients exclusively through their interactive website ("internet clients"), subject to a *de minimis* exception for other clients.[82] The Commission has stated that the internet investment adviser exemption was designed to balance the burdens of multiple state registration requirements for internet investment advisers with the Advisers Act's allocation of responsibility for regulating smaller advisers to state securities authorities.[83]

---

82 See 17 CFR 275.203A-2(e) (permitting Commission registration by an investment adviser that (i) provides investment advice to all of its clients exclusively through an interactive website, except that the investment adviser may provide investment advice to fewer than 15 clients through other means during the preceding twelve months; (ii) maintains specified records; and (iii) does not control, is not controlled by, and is not under common control with, another adviser that registers with the Commission solely because of its relationship with the internet investment adviser). Internet investment advisers represented only 1.5 percent of registered advisers in 2021, but have more than tripled in number since 2010—from 57 in 2010 (approximately 0.5 percent of total registered investment advisers) to 203 in 2021 (approximately 1.5 percent of total registered investment advisers). Data from Form ADV, Part 1A, Item 2.A.(11) (based on Form ADV filings through July 2021).

83 See Exemption For Certain Investment Advisers Operating through the Internet, Advisers Act Release No. 2091 (Dec. 12, 2002) [67 FR 77620, 77621 (Dec. 18, 2002)] ("Internet Investment Adviser Adopting Release") ("Because an Internet Investment Adviser uses an interactive Web site to provide investment advice, the adviser's clients can come from any state, at any time. As a result, Internet Investment Advisers must as a practical matter register in every state. This ensures that the adviser's registrations will be in place when it later obtains the requisite number of clients from any particular state" that requires state registration.).

For purposes of the exemption, "interactive website" means a website in which computer software-based models or applications provide investment advice to clients based on personal information each client supplies through the website. These websites generally require clients to answer questions about personal finances and investment goals, which the adviser's application or algorithm analyzes to develop investment advice that the website transmits to the client. The Commission has stated that the exemption is not available to investment advisers that merely use websites as marketing tools or use internet tools such as e-mail, chat rooms, bulletin boards, and webcasts or other electronic media in communicating with clients.[84] In addition, the Commission distinguished the interactive website described in the exemption from "other types of Web sites that aggregate and provide financial information in response to user-provided requests that do not include personal information."

This exemption is limited in scope. In the Internet Investment Adviser Adopting Release, the Commission stated that internet investment advisers typically are not eligible to register with the Commission because they "do not manage the assets of their Internet clients" and thus do not meet the statutory threshold for registration with the Commission. Further, the Commission stated that, in order to be eligible for registration under this exemption, an investment adviser "may not use its advisory personnel to elaborate or expand upon the investment advice provided by its interactive website, or otherwise provide investment advice to its Internet clients." The exemption generally requires that the investment adviser "provides investment advice to all of its clients" through its website, which means that the adviser must operate an interactive website

---

[84] Id. at n.15 and accompanying text. Effective September 19, 2011, Rule 203A-2(f) was renumbered as Rule 203A-2(e). See Rules Implementing Amendments to the Investment Advisers Act of 1940, Advisers Act Release No. 3221 (June 22, 2011) [76 FR 42950, 42963 (July 19, 2011)].

through which advice is given. That is, the exemption is unavailable to investment advisers lacking such a website.

Despite the limited nature of the exemption, we understand that some investment advisers may seek to rely on it and to register with the Commission without meeting the exemption's terms or intended purpose.[85] Examinations of investment advisers relying on the exemption have revealed various reasons for non-compliance with the exemption's requirements, including: (i) failure to understand the eligibility requirements; (ii) websites that were not interactive; (iii) businesses that became dormant but did not withdraw their registration; and (iv) client access to advisory personnel who could expand upon the investment advice provided by the adviser's interactive website, or otherwise provide investment advice to clients, such as financial planning.

Some robo-advisers may provide a broader array of advisory services than those provided by internet investment advisers but not be eligible for Commission registration unless they can rely on another exemption or until they have met the statutory assets-under-management threshold.[86] Prohibiting these investment advisers from registering with the Commission in these circumstances could impose burdens that the internet investment adviser exemption was intended to alleviate. Finally, because the internet investment adviser exemption was established almost twenty years ago, we seek to understand better how investment advisers are relying on it

---

85 The Commission has cancelled the registrations of advisers where the Commission found that those advisers did not meet the terms of the exemption. See, e.g., Order Cancelling Registration Pursuant to Section 203(h) of the Investment Advisers Act of 1940, Advisers Act Release No. 5110 (Feb. 12, 2019).

86 Some of these advisers also may be eligible for the "multi-state adviser exemption" under 17 CFR 275.203A-2(d). The multi-state adviser exemption permits an adviser who is required to register as an investment adviser with fifteen or more states to register with the Commission.

and whether we should consider amending the exemption or creating another exemption that reflects investment advisers' current use of technology in providing investment advice.

3. AI/ML in Developing and Providing Investment Advice.[87]

Investment advisers may use, or be considering the use of, software or models based on, or otherwise incorporating, AI/ML (including deep learning, supervised learning, unsupervised learning, and reinforcement learning) in developing and providing investment advice, including by supporting human personnel's decision-making.[88] Investment advisers may use such models or software to devise trading and investment strategies or develop investment advice, including to assess large amounts of data or to provide clients with more customized service.[89] In addition, investment advisers may use these tools to monitor client accounts or track the performance of specific securities or other investments.[90]

---

87 Investment advisers' use of AI/ML and other technological tools must comply with existing rules and regulations. The Commission is not expressing a view as to the legality or conformity of such practices with the federal securities laws and the rules and regulations thereunder, nor with the rules of self-regulatory organizations.

88 Advisers may also use AI as part of their internal operations, including by reviewing and classifying information (e.g., in regulatory filings and fund prospectuses), by assisting with trade matching or custodian reconciliation, for risk measurement (in part through earlier and more accurate estimation of risks) and stress testing purposes, and by facilitating regulatory compliance.

89 See, e.g., Treasury RFI, supra note 11, at 16839 (describing potential benefits of financial institutions' use of AI); see also FINRA AI Report, supra note 11 (highlighting three broad areas where broker-dealers are evaluating or using AI: communications with customers, investment processes, and operational functions); FSB AI Report, supra note 11, at 27.

90 Advisers may obtain these AI/ML tools in connection with contracting for cloud services. They may use other types of Fintech, as well, such as financial aggregator platforms that allow advisers to access information about clients' financial accounts, which can inform investment advice. Clients may allow such platforms to access information about their investment accounts and performance to enable a more fulsome analysis of their financial resources and investment experience.

Because ML models learn and develop over time, advisory personnel may face challenges in monitoring and tracking them, including reviewing both a model's input to assess whether it is appropriate and its output to assess accuracy or relevance.[91] For example, advisory personnel may lack sufficient knowledge or experience, or rely heavily on limited personnel, to challenge models' results. In addition, there may be systemic risks associated with the use of these technologies, including potential interconnectedness across the financial system and an emerging dependency on certain concentrated infrastructure and widely used models, which could propagate risks across the financial system. Further, different market participants may use technologies of varying or inadequate quality that could prompt investment advisers to provide unsuitable advice to their clients.

4. Potential Benefits.

The use of technology in developing and providing investment advice has provided certain benefits to investment advisers and, in turn, their clients. For example, digital advisers and internet investment advisers may offer lower cost advisory services. They also may provide attractive, user-friendly design features that clients appreciate, and may offer advisory services and online access at all hours of the day.[92] Digital investment advice may be more accessible than human advisory personnel to a wider range of clients, including clients who have greater confidence in digital investment advice; may facilitate access to a wider range of investment

---

91 See, e.g., IOSCO, The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers at 11 (June 2020) (consultation report), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD658.pdf ("Unlike traditional algorithms, ML algorithms continually learn and develop over time. It is important that they are monitored to ensure that they continue to perform as originally intended.").

92 See, e.g., Coryanne Hicks, What Is a Robo Advisor and When to Use One, U.S. News & World Report (Feb. 18, 2021), https://money.usnews.com/financial-advisors/articles/what-is-a-robo-advisor-and-when-to-use-one.

advisers, including through increased competition and a potential for lower fees; and may permit clients to easily access information about their account and investments.[93] In addition, digital advisers may be less prone to "behavioral biases, mistakes, and illegal practices" than human personnel.[94] By using AI-based software and methods, advisers may provide clients more customized advice or advice that benefits from analysis of more information (or types of information) on a more cost-effective basis than could be provided using traditional tools. In addition, investment advisers may use AI/ML to enhance and expand their services, generate investment strategies, and expand access to investment advice.[95] Clients may benefit from

---

93 See, e.g., European Securities and Markets Authority ("ESMA") et al., Joint Committee Discussion Paper on Automation in Financial Advice at 16-17 (Dec. 4, 2015) ("ESMA Discussion Paper"), https://esas-joint-committee.europa.eu/Publications/Discussion%20Paper/20151204_JC_2015_080_discussion_paper_on_Automation_in_Financial_Advice.pdf; see also ESMA et al., Report on Automation in Financial Advice at 8-9 (2016) ("ESMA Report"), https://esas-joint-committee.europa.eu/Publications/Reports/EBA%20BS%202016%20422%20(JC%20SC%20CPFI%20Final%20Report%20on%20automated%20advice%20tools).pdf (discussing views on the benefits and risks of automated advice from respondents to the ESMA Discussion Paper).

94 Söhnke M. Bartram, Jürgen Branke, and Mehrshad Motahari, Artificial Intelligence in Asset Management, CFA Institute Research Foundation Literature Review 25 (2020) ("CFA Literature Review"), https://www.cfainstitute.org/-/media/documents/book/rf-lit-review/2020/rflr-artificial-intelligence-in-asset-management.ashx; see also ESMA Discussion Paper, supra note 93, at 17 ("A well-developed algorithm may be more consistently accurate than the human brain at complex repeatable regular processes, and in making predictions. Automated advice tools therefore could reduce some elements of behavioural biases, human error, or poor judgement that may exist when advice is provided by a human. A well-developed algorithm could ensure equal and similar advice to all consumers with similar characteristics."). But see ESMA Report, supra note 93, at 9 (stating that several respondents "stated that whether or not automated advice is more consistent and accurate depends on both the underlying logic of the algorithm and the quality and completeness of the information inputted"); text accompanying infra note 97.

95 See, e.g., World Economic Forum, The New Physics of Financial Services: Understanding How Artificial Intelligence is Transforming the Financial Ecosystem 114-123 (Aug. 2018), http://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf.

investment advisers' ability to use this this technology to improve trade execution, as well. In addition, AI-based tools may substantially enhance efficiencies in information processing, reducing information asymmetries, and contributing to the efficiency and stability of markets.

5. Potential Risks.

At the same time, these developments may pose new or different risks to clients, including risks presented by investment advisers' reliance on technology and any third parties that provide or service such technology. For example, digital advisers may limit clients' access to human personnel, including when clients are considering major life changes such as retirement or when clients have questions that are highly fact-specific. Clients of internet investment advisers may have issues accessing the interactive websites, which can present unique challenges when the website is the sole means for advice delivery. The quality of the investment advice may depend on an algorithm that human personnel may monitor infrequently, incorrectly or face challenges overseeing.[96] The use of algorithms may be subject to their own risks, including risks related to the input data (such as a mismatch between data used for training the algorithm and the actual input data used during operations), algorithm design (such as flawed assumptions or judgments), and output decisions (such as disregard of underlying assumptions).[97] Digital advisers may encourage clients to trade more to the extent that the adviser integrates trade execution services, which may benefit the adviser at the expense of the client.[98] Depending on

---

96 See, e.g., In the Matter of AXA Rosenberg Group LLC et al., Advisers Act Release No. 3149 (Feb. 3, 2011) (settled action); see also In the Matter of Barr M. Rosenberg, Advisers Act Release No. 3285 (Sept. 22, 2011) (settled action) (finding, in part, that an adviser breached his fiduciary duty by directing others to keep quiet about, and delay fixing, a material error in computer code underlying his company's automated model).

97 See Deloitte Report, supra note 77, at 4.

98 See CFA Literature Review, supra note 94, at 25 ("At the same time, because robo-advisors have trade execution services integrated into them, they often encourage

the quality, recency, and thoroughness of a client's information incorporated into an algorithm, as well as how broadly client risk tolerances or investment goals are generalized by the algorithm, the use of algorithms may cause some clients to receive investment advice that is less individualized than they reasonably expect. Similarly, clients may face risks when AI/ML models use poor quality, inaccurate, or biased data that produces outputs that are or lead to poor or biased advice. In this respect, biased data may be incorporated unintentionally through use of data sets that include irrelevant or outdated information, including information that exists due to historical practices or outcomes, or through the selection by human personnel of the data or types of data to be incorporated into a particular algorithm.[99]

To the extent that a third party, rather than the investment adviser, develops the analytical tools, the adviser may face challenges in understanding or overseeing those third parties or the technology. For example, there may be challenges in cases where software or a model is based on an approach or technology that is proprietary to the third party or is hosted by a third party, or where the investment adviser's personnel do not have the knowledge or experience necessary to understand the technology or to challenge its results. These circumstances may exacerbate exposure of investment advisers and their clients to cybersecurity and data privacy risks.

---

investors to trade more. This increased trading can be both a benefit, in terms of encouraging investors to rebalance positions more often, and a pitfall, because it can lead to excessive trading that benefits robo-advising systems through commissions at the expense of investors.").

99 See FINRA AI Report, supra note 11, at 14; see also Treasury RFI, supra note 11, at 16840 ("Because the AI algorithm is dependent upon the training data, an AI system generally reflects any limitations of that dataset. As a result, as with other systems, AI may perpetuate or even amplify bias or inaccuracies in the training data, or make incorrect predictions if that data set is incomplete or non-representative."); Jessica Fjeld et al., Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI 47-49 (Berkman Klein Center for Internet & Society at Harvard University, Research Publication, 2020).

Further, these risks may affect more clients than those posed by investment advisers using traditional methods because of the scale at which investment advisers are able to reach clients through digital platforms.

Clients' ability to understand these and other risks rests on the quality and sufficiency of their investment advisers' disclosures, which may be particularly important to the extent that these developments reflect the use of underlying technology that is complex or otherwise requires technical expertise. Disclosure can put clients in a position to understand the different roles played by technology and advisory personnel in developing the investment advice that clients receive. Investment advisers may face challenges in disclosing sufficiently these types of risks where any such disclosure might be necessarily technical.

There may also be systemic risks associated with widespread use of AI/ML, including deep learning, supervised learning, unsupervised learning, and reinforcement learning, which may affect the maintenance of fair, orderly, and efficient markets. For example, the Financial Stability Board has stated that "applications of AI and machine learning could result in new and unexpected forms of interconnectedness between financial markets, for instance based on the use by various institutions of previously unrelated data sources."[100] In addition, there could be systemic risk to the extent that digital advisers employ models (including models from third-party model providers) that rely on past performance and volatility, which could constitute input data that is inappropriate for the current market. These and other risks may continue to grow as the use of AI continues to increase among investment advisers.

We request comment on all aspects of investment advisers' use of technology, particularly with respect to developing and providing investment advice, and the potential effect

---

100 FSB AI Report, supra note 11, at 1.

on investor protection and regulatory compliance. We specifically request comment on the following:

4.1 How do investment advisers currently use technology in developing and providing investment advice? What types of technology do advisers use for these purposes? How do investment advisers use technology in any quantitative investment processes that they employ?

4.2 Are our descriptions of the potential benefits and risks of investment advisers' use of technology in developing and providing investment advice accurate and comprehensive? If not, what additional benefits or risks to advisory clients are there from such use? What additional benefits or risks does using these types of technology provide to investment advisers? How do investment advisers weigh these benefits and risks in using technology to develop and provide investment advice? Does technology enable investment advisers to develop investment advice in a more cost-effective way and are clients able to receive less expensive advice as a result? Does technology increase access to investment advice for some clients who would otherwise not afford it or mitigate (or have the potential to mitigate) biases in the market that may have prevented access to some clients or prospective clients? Are there risks associated with the quality of services clients ultimately receive? If so, what are they and how do investment advisers address such risks? What factors do advisory clients consider in choosing to engage a robo-adviser rather than a traditional investment adviser? In what ways does investment advice developed or provided by a robo-adviser differ from investment advice developed or provided by a traditional investment adviser?

4.3 To the extent investment advisers use technology in developing and providing investment advice, do advisers assess whether the technology or its underlying models are explainable to advisory personnel or to clients? Is the technology or underlying model explainable? To what extent do investment advisers assess whether the results are reproducible? If so, are the results reproducible? To what extent do investment advisers rely on third parties to make these assessments?

4.4 How do investment advisers develop, test, deploy, monitor, and oversee the technology they use to develop and provide investment advice? Do investment advisers develop, test, and monitor AI/ML models differently from how they develop, test, and monitor traditional algorithms? How do investment advisers assess the effect on client accounts of any material change to advisers' technology, algorithm, or model prior to implementation? Do investment advisers communicate with clients about such material changes? If so, how?

4.5 What, if anything, do investment advisers do to understand how AI/ML models will operate during periods of unusual or volatile market activity or other periods where such models may have less, or less relevant, input data with which to operate? How does the use of these models by investment advisers affect the market more generally? What formal governance mechanisms do investment advisers have in place for oversight of the vendors that create or manage these models?

4.6 How do investment advisers disclose the use of algorithms or models to their clients, including the role of advisory personnel or third parties in creating and managing these algorithms or models? Do these disclosures address any effects that such use may have on client outcomes? When investment advice is developed and provided

through an automated algorithm, how do advisers disclose the use of that automated algorithm? Do investment advisers assess how effective these disclosures are in informing clients about such use? If so, how effective are such disclosures? Please provide any available data to show how effective such disclosures are. What are clients' expectations for investment advice produced by an investment adviser's automated algorithm, and how are those expectations shaped by investment advisers' disclosures?

4.7 How do investment advisers account for the use of any poor quality, inaccurate, or biased data that are used by AI/ML models, and how do investment advisers determine the effect of this kind of data on the algorithms' output or seek to reduce the use of this kind of data? To what extent can the use of AI/ML models in developing investment advice perpetuate social biases and disparities? How have commenters seen this in practice with regard to the use of AI/ML models (e.g., through marketing, asset allocation, fees, etc.)? To what extent and how do investment advisers employ controls to identify and mitigate any such biases or disparities? For example, do investment advisers evaluate the output of their models to identify and mitigate biases that would raise investor protection concerns? Do investment advisers utilize human oversight to identify biases that would raise investor protection concerns, in both the initial coding of their models or in the resulting output of those models?

4.8 Are there any particular challenges or impediments that investment advisers face in using AI/ML to develop and provide investment advice? If so, what are they and how

do investment advisers address such challenges or impediments and any risks associated with them?

4.9 When relying on AI/ML models to develop investment advice, how do advisers determine whether those models are behaving as expected? How do advisers verify the quality of the assumptions and methodologies incorporated into such models? How frequently do advisers test these models? For example, do advisers test a model each time it is updated? What model risk management steps should advisers undertake? What is advisers' understanding of their responsibility to monitor, test, and verify model outputs? How do advisers' approaches with respect to AI/ML models differ from other models that advisers may use in developing investment advice?

4.10 In the context of developing and providing investment advice, what is the objective function of AI/ML models (e.g., revenue generation)? What are the inputs relied on by AI/ML models used in developing and providing investment advice (e.g., visual cues or feedback)? Does the ability to collect individual-specific data impact the effectiveness of the AI/ML model in maximizing its objective functions?

4.11 What cybersecurity and data security risks result from investment advisers' use of technology in developing and providing investment advice? How do investment advisers address or otherwise manage those risks and how do investment advisers disclose these risks to clients? Do investment advisers believe that delivering investment advice through email, which may be encrypted, is more secure than delivery through online client portals? Conversely, do investment advisers believe

that delivery through online client portals is more secure? How do investment advisers address these concerns when clients are using mobile apps?

4.12 How do investment advisers generate records to support the investment advice they develop from using these types of technology? What types of records do they produce and how do investment advisers retain them? Does an investment adviser's recordkeeping process differ based on the type of technology it uses? If so, how?

4.13 Do investment advisers generate and retain records with respect to the testing of, or due diligence with respect to, the technology that they use in developing and providing investment advice?

4.14 To what extent do investment advisers market the types of technology the adviser uses in developing and providing investment advice? To the extent investment advisers market their use of technology, do advisers demonstrate that use to clients? To what extent do prospective and existing clients seek to assess investment advisers' understanding of the technology, or seek to understand the technology for themselves, in determining whether to hire or retain an investment adviser? If prospective or existing clients make such an assessment, how do they do so?

4.15 How do investment advisers disclose the types of technology used in developing and providing investment advice? What types of potential risks and conflicts of interest are disclosed? How are fees disclosed? To what extent does investment advisers' use of technology produce conflicts of interest that are similar to those of investment advisers that do not use such technologies? To what extent does investment advisers' use of technology produce conflicts that result from such use?

4.16 In what ways do investment advisers assess whether using these types of technology to develop and provide investment advice enables them to satisfy their fiduciary duty to their clients? How do investment advisers assess their ability to satisfy their duty of care and duty of loyalty when using these types of technology? How does an investment adviser determine whether the advice produced by its automated algorithm is in the best interest of a particular client? To what extent and how often do advisory personnel review investment advisers' algorithms to be sure that such advice is in the client's best interest? In conducting such review, to what extent do advisory personnel understand the algorithm, how it was created, and how it operates in practice? How do advisers take into account their fiduciary duty when developing, testing, monitoring, and overseeing these types of technology? To what extent do investment advisers rely on technology vendors or other third parties to provide technical knowledge so that advisers can understand the algorithms and the information or analysis they generate? When relying on such vendors or third parties, how do investment advisers assess whether the investment advisers are able to satisfy their duty of care and duty of loyalty?

4.17 What types of policies and procedures do investment advisers maintain with respect to the technologies they use in developing and providing investment advice to clients? For example, do these investment advisers maintain policies and procedures under rule 206(4)-7 of the Advisers Act that are designed to address the technologies that they use or provide to clients? How do investment advisers' policies and procedures address their use of technology and the duties they owe their clients? Do they address how advisers determine how to incorporate information or analysis developed by

these types of technologies into investment advice that satisfies their fiduciary duty? If so, how? How do investment advisers introduce new technology to their personnel?

4.18 What types of operational risks do investment advisers face using digital platforms to interact with clients? How do investment advisers interact with clients when the platform is unavailable—for example, when the adviser has lost internet service or when the platform is undergoing maintenance? What alternative means of communication are available to clients during those times? When issues arise, is the investment adviser responsible to the client for resolving those issues, or does the investment adviser rely on others to resolve the issues or to be responsible to the client? What terms of service do investment advisers put in place with cloud service providers in connection with the potential for loss of service or loss of data? We understand that investment advisers, like other financial services companies, may rely on a small number of cloud service providers.[101] What risks does this reliance present to the industry (and advisory clients)?

4.19 Under what circumstances do robo-advisers typically override their algorithm, and in what ways? What steps do robo-advisers take to ensure that any override of the algorithm is consistent with the adviser's disclosure and clients' best interest? Do robo-advisers document their determinations to override the algorithm and, if so,

---

[101] See, e.g., Sophia Furber, As 'Big Tech' Dominates Cloud Use for Banks, Regulators May Need to Get Tougher, S&P Global (Aug. 18, 2020), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/as-big-tech-dominates-cloud-use-for-banks-regulators-may-need-to-get-tougher-59669007.

what specifically is documented? What have robo-advisers found to be the outcomes from overriding an algorithm?

4.20 When evaluating digital platforms, how do investment advisers weigh the platform's cost and quality of service?

4.21 Should the Commission consider amending Form ADV to collect information about the types of technology that advisers use to develop and provide investment advice? If so, what type of technology and why? What information about technology should we consider collecting? Should the Commission require investment advisers to describe their efforts to monitor the outputs of technology upon which they rely? Should the Commission consider another method of collecting this information?

4.22 What costs or benefits do investment advisers experience in registering with the Commission under the exemption for internet investment advisers? What costs or benefits do clients of internet investment advisers experience as compared to clients of other investment advisers registered with the Commission? Do commenters believe that the exemption for internet investment advisers should be updated in any way, including to facilitate its use or to modernize it? Are its conditions appropriate? Should we consider changes to, for example, the *de minimis* exception for non-internet clients or the recordkeeping requirement? Should we consider changes to the exemption's definition of "interactive website"? Should the exemption specify what it means to provide investment advice "exclusively" through the interactive website? Would additional guidance on any of the exemption's conditions or definitions be useful?

4.23 The Commission has stated that an investment adviser relying on the internet investment adviser exemption "may not use its advisory personnel to elaborate or expand upon the investment advice provided by its interactive Web site, or otherwise provide investment advice to its internet clients."[102] Should the Commission consider eliminating or modifying this language? Should the Commission consider changes to the exemption that reflect or otherwise address this language? Should the Commission provide additional guidance about the internet investment adviser exemption?

4.24 As discussed above, the Commission acknowledged that the internet investment adviser exemption was designed to balance these advisers' multiple state registration requirements with the Advisers Act's allocation of responsibility for regulating smaller advisers to state securities authorities. Consistent with this design, are there changes to the exemption that might help to ensure that it encompasses those investment advisers that provide advice through the internet while ensuring that advisers that use the internet only as a marketing tool, for example, remain subject to state registration? Should the Commission consider creating a registration exemption that reflects investment advisers' current use of technology in providing investment advice in a better way than the internet investment adviser exemption?

4.25 To what extent do investment advisers use digital platforms and other analytical tools in connection with wrap fee programs?[103] For example, do these programs use model

---

102 Internet Investment Adviser Adopting Release, supra note 83, at 77621.

103 In a wrap fee program, clients generally are charged one fee in exchange for investment advisory services, the execution of transactions, and custody (or safekeeping) as well as other services. An adviser acting as a sponsor to such a program may choose the service

portfolios or portfolio allocation models (whether developed by the investment adviser or by a third party that provides such models to the adviser for its use) to recommend investor allocations?[104] Do wrap fee programs with an online presence allow clients to engage directly with the portfolio manager managing the client's assets or provide access to a wider array of service providers than the client might otherwise have? Are there concerns with respect to these programs for clients with minimal or no trading activity as commissions for trade execution have moved toward zero?[105] Are such concerns different for wrap fee programs sponsored by robo-advisers as compared to those sponsored by traditional investment advisers?

---

providers, including other investment advisers, and provide clients with access to those services through internet-based platforms that enable clients to engage directly with service providers.

104 A model portfolio generally consists of a diversified group of assets (often mutual funds or ETFs) designed to achieve a particular expected return with exposure to corresponding risks that are rebalanced over time. See Morningstar, 2020 Model Portfolio Landscape (2020) (noting that, while models can focus on a single asset class, most models combine multiple asset classes). Model portfolios are distinct from portfolio allocation models, which can be educational tools that investors use to obtain a general sense of which asset classes (as opposed to which specific securities) are appropriate for the investor to allocate its assets to (e.g., appropriate balance of equities, fixed income, and other assets given age and other facts and circumstances).

105 See generally Securities and Exchange Commission, Division of Examinations, Risk Alert: Observations from Examinations of Investment Advisers Managing Client Accounts That Participate in Wrap Fee Programs (July 21, 2021), at 4 ("Infrequent trading in wrap fee accounts was also identified at several examined advisers, raising concerns that clients whose wrap fee accounts are managed by portfolio managers with low trading activity are paying higher total fees and costs than they would in non-wrap fee accounts."), https://www.sec.gov/files/wrap-fee-programs-risk-alert_0.pdf. The Risk Alert represents the views of the staff of the Division of Examinations. It is not a rule, regulation, or statement of the Commission. The Commission has neither approved nor disapproved its content. The Risk Alert, like all staff statements, has no legal force or effect: it does not alter or amend applicable law, and it creates no new or additional obligations for any person.

4.26 To what extent do robo-advisers (as well as other sponsors of investment advisory programs) rely on Rule 3a-4 to determine that they are not sponsoring or otherwise operating investment companies under the Investment Company Act of 1940 (the "Investment Company Act")?[106] If such sponsors do not rely on the rule, what policies and practices have sponsors adopted to prevent their investment advisory programs from being deemed to be investment companies?

4.27 To satisfy the conditions of Rule 3a-4, among other things, a sponsor and personnel of the manager of the client's account who are knowledgeable about the account and its management must be reasonably available to the client for consultation. The rule does not dictate the manner in which such consultation with clients should occur. How do sponsors and other advisers satisfy this condition? Should we consider amending Rule 3a-4 to address technological developments, such as chatbots and/or other responsive technologies providing novel ways of interacting with clients? Should the Commission address these developments in some other way? Should the Commission provide additional guidance about this condition? If yes, what specifically should this guidance address?

---

106 See 17 CFR 270.3a-4. Certain discretionary investment advisory programs may meet the definition of "investment company" under the Investment Company Act, but the Commission has indicated that investment advisory programs that provide each client with individualized treatment and the ability to maintain indicia of ownership of the securities in their accounts are not investment companies. Whether such a program is an investment company is a factual determination and depends on whether the program is an issuer of securities under the Investment Company Act and the Securities Act. Rule 3a-4 under the Investment Company Act provides a non-exclusive safe harbor from the definition of "investment company" to investment advisory programs that are organized and operated in the manner provided in the rule. A note to the rule also states that there is no registration requirement under Section 5 of the Securities Act for programs that rely on the rule, and that the rule is not intended to create any presumption about a program that does not meet the rule's provisions.

4.28 To satisfy the conditions of Rule 3a-4, among other things, each client's account must be managed on the basis of the client's financial situation and investment objectives. Sponsors must obtain information from each client about their financial situation and investment objectives at account opening and must contact each client at least annually thereafter to determine whether there have been any changes in the client's financial situation or investment objectives. The Commission stated that the receipt of individualized advice is "one of the key differences between clients of investment advisers and investors in investment companies."[107] How do sponsors ensure that they have sufficient information about a client's financial situation and investment objectives to provide investment advice that is in the best interest of the client, including advice that is suitable for the client? Given the availability of new technology for developing and providing investment advice, does a sponsor's reliance on Rule 3a-4 heighten the risk of clients receiving unsuitable advice? If so, are there other requirements or conditions that might address this risk?

4.29 One of the conditions of Rule 3a-4 is that investment advisory programs relying on the rule be managed in accordance with any reasonable restrictions imposed by the client on the management of the client's account. In addition, the client must have the opportunity to impose reasonable restrictions at the time the account is opened

---

[107] See Status of Investment Advisory Programs under the Investment Company Act of 1940, Investment Company Act Rel. No. 21260 (July 27, 1995), 60 FR 39574 (Aug. 2, 1995). The Commission also stated that to fulfill its duty to provide only suitable investment advice, "an investment adviser must make a reasonable determination that the investment advice provided is suitable for the client based on the client's financial situation and investment objectives. The adviser's use of a model to manage client accounts would not alter this obligation in any way." See Status of Investment Advisory Programs under the Investment Company Act of 1940, Investment Company Act Rel. No. 22579 (Mar. 24, 1997), 62 FR 15098 (Mar. 31, 1997).

and must be asked at least annually whether the client might wish to impose any reasonable restrictions or reasonably modify existing restrictions. The Commission explained that the ability of a client to impose reasonable restrictions on the management of a client account is a critical difference between a client receiving investment advisory services and an investor in an investment company. Since the rule was adopted, enhanced technological capabilities and industry practices may have made it practical for sponsors to provide clients with other means of receiving meaningful individualized treatment regarding the management of their accounts. Do sponsors of investment advisory programs currently provide their clients with ways of customizing or personalizing their accounts other than through the imposition of reasonable restrictions? If yes, please provide examples of such practices. To what extent do clients avail themselves of those options for individualized treatment and do they find them to be valuable or important? Should we consider amending Rule 3a-4 to address these developments or should we address them in some other way, such as by providing additional guidance about this condition?

4.30 In view of the variety and increasing availability of technologies used by investment advisers to develop and provide investment advice, are there other regulatory matters that the Commission should consider? If so, what are they, and why? To the extent commenters recommend any modifications to existing regulations or additional regulations, what economic costs and benefits do commenters believe would result from their recommendations? Please provide or identify any relevant data and other information.

IV. GENERAL REQUEST FOR COMMENT

This Request is not intended to limit the scope of comments, views, issues, or approaches to be considered. In addition to broker-dealers, investment advisers and investors, we welcome comment from other interested parties, researchers and particularly welcome statistical, empirical, and other data from commenters that may support their views or support or refute the views or issues raised by other commenters.

By the Commission.

Dated: August 27, 2021.

Vanessa A. Countryman,

Secretary.

Appendix A

Tell Us about Your Experiences with Online Trading and Investment Platforms

We're asking individual investors like you what you think about online trading or investment platforms such as websites and mobile applications ("apps"). It's important to us at the SEC to hear from investors who trade and invest this way so we can understand your experiences.

Please take a few minutes to answer any or all of these questions. Please provide your comments on or before October 1, 2021 - and thank you for your feedback!

1. Do you have one or more online trading or investment accounts?

- o Yes, I have one or more accounts that I access online using a computer.
- o Yes, I have one or more accounts that I access using a mobile app.
- o Yes, I have one or more accounts that I access both online using a computer and using a mobile app.
- o Yes, I have one or more accounts that I access online, either using a computer or a mobile app, but I also access the account(s) in other ways (e.g., by calling or visiting in person).
- o I have one or more accounts, but I do not access them online using a computer or using a mobile app.
- o No, I don't have a trading or investment account.

2. If your response to Question 1 is "Yes", do you think you would trade or invest if you could not do so online using a computer or using a mobile app?

- o Yes
- o No

3. On average, how often do you access your online account?

- o Daily/more than once a day
- o Once to a few times a week
- o Once to a few times per month
- o Less often than once a month
- o Never
- o Other

If Other, Explain:

4. On average, how often are trades made in your online account, whether by you or someone else?

- o Daily/more than once a day
- o Once to a few times a week
- o Once to a few times per month
- o Less often than once a month
- o Never
- o Other

If Other, Explain:

5. If you access your account online, did you have the account first, and only began to access it electronically later? Or did you open the account with the idea that you would access it electronically immediately?

- o I had a pre-existing account and downloaded an app or visited a website to access my account.
- o I downloaded an app or visited a website first, and then opened up an account with the company.

6. My goals for trading or investing in my online account are (check all that apply):

- □ Keep the amount of money I have, while keeping up with inflation
- □ Save and grow my money for short-term goals (in the next year or two)
- □ Save and grow my money for medium- to long-term goals
- □ Have fun
- □ Other

If Other, Explain:

7. What would you like us to know about your experience with the features of your online trading or investment platform? (Examples of features are: social networking tools; games, streaks, or contests with prizes; points, badges, and leaderboards; notifications; celebrations for trading; visual cues, like changing colors; ideas presented at order placement or other curated lists or features; subscription and membership tiers; or chatbots.)

8. If you were trading or investing prior to using an online account, how have your investing and trading behaviors changed since you started using your online account? (For example, the amount of money you have invested, your interest in learning about investing and saving for retirement, the amount of time you have spent trading, your knowledge of financial products, the number of trades you have made, the amount of money you have made in trading, your knowledge of the markets, the number of different types of financial products you have traded, or your use of margin.)

9. How much experience do you have trading or investing in the following products (None, Less than 12 months, 1-2 years, 2-5 years, 5+ years):

Investment Products	None	Less than 12 Months	1-2 Years	2-5 Years	5+ Years
Stocks	o	o	o	o	o
Bonds	o	o	o	o	o
Options	o	o	o	o	o
Mutual Funds	o	o	o	o	o
ETFs	o	o	o	o	o
Futures	o	o	o	o	o
Cryptocurrencies	o	o	o	o	o
Commodities	o	o	o	o	o
Closed-End Funds	o	o	o	o	o
Money Market Funds	o	o	o	o	o
Variable Insurance Products	o	o	o	o	o
Business Development Companies	o	o	o	o	o
Unit Investment Trusts	o	o	o	o	o

10. What is your understanding, if any, of the circumstances under which trading or investing in your account can be suspended or restricted?

11. What else would you like us to know – positive or negative - about your experience with online trading and investing?

Other Ways to Submit Your Feedback

You also can send us feedback in the following ways (include the file number S7-10-21 in your response):
Print Your Responses and Mail Secretary Securities and Exchange Commission 100 F Street, NE Washington, DC 20549-1090
Print a PDF of Your Responses and Email Use the printer-friendly page and select a PDF printer to create a file you can email to: rule-comments@sec.gov
Print a Blank Copy of this Flyer, Fill it Out, and Mail Secretary Securities and Exchange Commission 100 F Street, NE Washington, DC 20549-1090

Contact Info (Not required; to submit anonymously, leave blank)

First Name: _____ Last Name:_____

We will post your feedback on our website. Your submission will be posted without change; we do not redact or edit personal identifying information from submissions. You should only make submissions that you wish to make available publicly.

If you are interested in more information on the proposal, or want to provide feedback on additional questions, click here. Comments should be received on or before October 1, 2021.

Thank you!

Brokers With a Significant History of Misconduct
Tuesday, May 17, 2022
1:45 p.m. – 2:45 p.m.

Join FINRA staff as they discuss the new rules concerning brokers with significant history of misconduct. Panelists review the implications of retaining or hiring brokers with such a history.

Moderator:
Michael Garawski
Associate General Counsel, Regulatory
FINRA Office of General Counsel

Panelists:
Patricia Dorilio
Senior Director, Capital Markets Membership Application Program
FINRA Member Supervision

Jennifer Crawford
Vice President, Litigation
FINRA Enforcement

Eric Hebert
Director, High Risk Registered Representative Program
FINRA Member Supervision

Brokers With a Significant History of Misconduct Panelists Bios:

Moderator:

Michael Garawski is Associate General Counsel, Regulatory Practice & Policy, with FINRA's Office of General Counsel. In this role, Mr. Garawski directs and manages the complete life cycle of the adoption of new regulatory requirements, and he advises the FINRA Board of Governors, FINRA advisory committees, and senior FINRA management on regulatory initiatives and rule changes. Previously, he served as Associate General Counsel in FINRA's Appellate Group and as Assistant General Counsel with the Commodity Futures Trading Commission. He is a graduate of Boston College and the George Washington University Law School.

Panelists:

Patricia Dorilio became Senior Director in the Membership Application Program (MAP) group in November 2021 as lead of the Capital Markets firm group where, as a member of the MAP leadership team, she is responsible for the management and assessment of membership applications, as well as leading and implementing the strategic direction of the MAP program for the Capital Markets firm groupings. Prior to becoming a Senior Director, Ms. Dorilio was an Associate Director in the MAP group where she oversaw a team of managers and examiners in the execution of the application review program, including expedited reviews where applicable, to determine applicants' satisfaction of standards for FINRA membership, and standards for firms' continuation of membership. That included the review and analysis of information and documentation relating to proposed business activities and securities products, and firms' structural and ownership changes. She has also completed the FINRA Excellence in Management Program at Wharton. Prior to joining MAP in 2011 as a MAP examiner, Ms. Dorilio was employed in the private sector, and immediately prior to that, held the position of Senior Special Counsel at the New York Stock Exchange. She began her career as an Assistant Attorney General in the New York State Attorney General's Office. Ms. Dorilio earned her Juris Doctor from the Maurice A. Dean School of Law at Hofstra University, and a B.A. in Political Science from Hofstra University. She is a member of the bar of the State of New York.

Jen Crawford is Vice President of Litigation in the Enforcement Department, responsible for overseeing Enforcement's nationwide litigation and appellate programs. Prior to assuming this role, she was a Hearing Officer in FINRA's Office of Hearing Officers. Ms. Crawford joined FINRA in 2012 and was a Director in Enforcement until 2018. Prior to joining FINRA, she was a Senior Counsel in the Division of Enforcement at the U.S. Securities and Exchange Commission where she investigated and litigated enforcement matters in federal court and in administrative proceedings. Ms. Crawford holds a B.S. in Finance from Seton Hall University and J.D. from Catholic University.

Eric Hebert is Investigative Director with FINRA's High Risk Registered Representatives specialist team and has been with FINRA since December 2003. In his role, Mr. Hebert manages specialized staff performing assessments and examinations of registered persons deemed to present heighted risk to investors and the markets. Mr. Hebert started his career in Member Supervision as an Examiner with NASD. Prior to joining NASD/FINRA, Mr. Hebert was a Supervisory Principal for MetLife and New England Securities, and responsible for approving securities investment applications and transactions for an OSJ branch office. Mr. Hebert has a Bachelor of Arts degree from Curry College and is a Certified Fraud Examiner.

Brokers With a Significant History of Misconduct

Panelists

- **Moderator**
  - Michael Garawski, Associate General Counsel, Regulatory, FINRA Office of General Counsel
- **Panelists**
  - Patricia Dorilio, Senior Director, Capital Markets Membership Application Program, FINRA Member Supervision
  - Jennifer Crawford, Vice President, Litigation, FINRA Enforcement
  - Eric Hebert, Director, High Risk Registered Representative Program, FINRA Member Supervision

Road Map for Discussion

- New FINRA Rules and Amendments
- Disciplinary Proceedings Rules
- Membership Proceedings Rules
- Expedited Proceedings Rules
- Eligibility Proceedings Rules
- BrokerCheck Rule
- Other General Considerations

To Access Polling

- **Please get your devices out:**
  - Type the polling address, **https://finra.cnf.io/sessions/x9ya** into the browser or scan the QR code with your camera.

  - Select your polling answers.

Polling Question 1

1. **What size member firm do you work for?**
   a. Large member firm
   b. Mid-size member firm
   c. Small member firm
   d. Other (do not work for a member firm)

Polling address: **https://finra.cnf.io/sessions/x9ya**

Polling Question 2

2. What is your firm's grouping?

a. Retail
b. Capital Markets
c. Carrying and Clearing
d. Trading and Execution
e. Diversified
f. Don't know, what's a firm grouping?

Polling address: **https://finra.cnf.io/sessions/x9ya**

Polling Question 3

3. **What is your level of familiarity with the new rules concerning brokers with a significant history of misconduct?**
   a. I'm already familiar with the new rules.
   b. I'm somewhat familiar with the new rules.
   c. I'm not familiar with the new rules.

Polling address: **https://finra.cnf.io/sessions/x9ya**

Polling Question 4

4. Do you have any experience in working with any of the new rules concerning brokers with a significant history of misconduct?
   a. Yes
   b. No

Polling address: **https://finra.cnf.io/sessions/x9ya**

Polling Question 5

5. Have the new amendments to the MAP rules already impacted your work in anyway?
   a. Yes
   b. No

Polling address: **https://finra.cnf.io/sessions/x9ya**

Key Resources

- FINRA *Regulatory Notice 21-09*
- FINRA *Regulatory Notice 18-15*
- Key Topic Page – Protecting Investors from Misconduct

Brokers With a Significant History of Misconduct
Tuesday, May 17, 2022
1:45 p.m. – 2:45 p.m.

Resources:

- Key Topic Page: Protecting Investors from Misconduct

  www.finra.org/rules-guidance/key-topics/protecting-investors-from-misconduct

- FINRA *Regulatory Notice 21-09, FINRA Adopts Rules to Address Brokers With a Significant History of Misconduct* (March 2021)

  www.finra.org/rules-guidance/notices/21-09

- FINRA *Regulatory Notice 18-15, Guidance on Implementing Effective Heightened Supervisory Procedures for Associated Persons With a History of Past Misconduct* (April 2018)

  www.finra.org/rules-guidance/notices/18-15

- FINRA *Regulatory Notice 18-17, FINRA Revises the Sanction Guidelines* (May 2018)

  www.finra.org/rules-guidance/notices/18-17

- Mapping of Disclosure Categories for FINRA Rule 1017(a)(7)

  www.finra.org/sites/default/files/2021-04/mapping-disclosure-categories-rule-1017a7.pdf

- Checklist for Mandatory Materiality Consultations Under FINRA Rule 1017(a)(7)

  www.finra.org/rules-guidance/guidance/materiality-consultation-process/checklist-under-rules-1017a6_a7#1017_a_7

- FINRA Taping Rule (FINRA Rule 3170)

  www.finra.org/rules-guidance/guidance/taping-rule

- General Information on Statutory Disqualification and FINRA's Eligibility Proceedings

  www.finra.org/rules-guidance/guidance/eligibility-requirements

- Interim Plans of Heightened Supervision FAQs

  www.finra.org/sites/default/files/2021-06/HSP-interim-faq.pdf

- Sample Interim Plan of Heightened Supervision

  www.finra.org/sites/default/files/2021-06/HSP-interim-sample.pdf

Consolidated Audit Trail (CAT)
Tuesday, May 17, 2022
3:00 p.m. – 4:00 p.m.

During this session, panelists discuss how to prepare for compliance with the consolidated audit trail (CAT), including firm obligations, deadlines and resources.

Moderator:
David Chapman
Vice President, Market Analysis and Audit Trail Group
FINRA Market Regulation

Panelists:
Shelly Bohlin
President and Chief Operating Officer, FINRA CAT, LLC
FINRA CAT, LLC

Doug Pratt
Senior Director, CAT Compliance Surveillance & Investigations
FINRA Market Regulation

Peter Stoehr
Vice President, Trading and Execution (T&E) Examinations
FINRA Market Regulation

Consolidated Audit Trail (CAT) Panelists Bios:

Moderator:

David Chapman is Vice President in the Market Regulation Department of FINRA where he manages the Market Analysis and Audit Trail teams. These teams are responsible for conducting investigations regarding various reporting and market structure rules. Prior to this position, Mr. Chapman managed the Market Manipulation Investigations and Trading Systems teams, where he led investigations into various market-based manipulative activities. Mr. Chapman has worked in the financial services industry for 29 years and has been with FINRA for the last 25 years. Mr. Chapman earned a B.B.A. in Accounting, M.S. in Finance, both from Loyola University Maryland, and a J.D. from the Columbus School of Law at Catholic University.

Panelists:

Shelly Bohlin is President and Chief Operating Officer of FINRA CAT LLC, a subsidiary of FINRA that is the Plan Processor for the Consolidated Audit Trail (CAT). She also co-chairs the CAT Industry Member Technical Specifications Working Group. In addition, Ms. Bohlin served on the CAT Plan Participant Leadership Team until FINRA was selected as the CAT Plan Processor. Previously, Ms. Bohlin was Vice President in the Quality of Markets Section of FINRA's Market Regulation Department. She oversaw the Market Analysis and Audit Trail Group, which is responsible for monitoring member-firm compliance with FINRA rules and federal securities laws related to market making, order handling, trade reporting and FINRA's Order Audit Trail System (OATS). She is a Certified Public Accountant and has a B.S.B.A. in Finance and Accounting from the University of Arkansas.

Doug Pratt is Senior Director in the Quality of Markets group within FINRA's Market Regulation Department. Mr. Pratt oversees the CAT Compliance Team which conducts surveillance to ensure Industry Member compliance with the various reporting requirements of the Consolidated Audit Trail. Mr. Pratt served in a similar role within Market Regulation as the Senior Director of the Order Audit Trail System (OATS) Compliance Team until OATS was retired last year. Before joining FINRA in 2007, Mr. Pratt worked in the surveillance department of a small broker dealer, drafting internal compliance procedures and conducting onsite examinations of branch offices to ensure adherence to FINRA rules. Prior to that, Mr. Pratt spent nearly seven years as an over-the-counter position trader for Raymond James Financial at their home office in Florida. Mr. Pratt earned his Bachelor of Science Degree in Finance from the University of Florida

Peter G. Stoehr is Vice President of the Trading and Execution Firm Group ("T&E") within FINRA's Market Regulation Department. T&E conducts equities, options, fixed income, and financial operations cycle examinations as well as for-cause examinations for compliance with FINRA, SEC and Exchange related trading rules and regulations. Mr. Stoehr is responsible for the management of the T&E Options, Equities, Trading Specialist Group, and For-Cause Examination Program. He has been with FINRA since 1997 and prior to that was employed at Pershing LLC.

Consolidated Audit Trail (CAT)

Panelists

- **Moderator**
  - David Chapman, Vice President, Market Analysis and Audit Trail Group, FINRA Market Regulation
- **Panelists**
  - Shelly Bohlin, President and Chief Operating Officer, FINRA CAT, LLC
  - Doug Pratt, Senior Director, CAT Compliance Surveillance & Investigations, FINRA Market Regulation
  - Peter Stoehr, Vice President, Trading and Execution (T&E) Examinations, FINRA Market Regulation

Consolidated Audit Trail (CAT)
Tuesday, May 17, 2022
3:00 p.m. – 4:00 p.m.

Resources:

- FINRA *Regulatory Notice 20-31, FINRA Reminds Firms of Their Supervisory Responsibilities Relating to CAT* (August 2020)

  www.finra.org/rules-guidance/notices/20-31

- 2022 Report on FINRA's Examination and Risk Monitoring Program (Section on CAT)

  www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program/cat

- CAT CAIS Implementation Timeline

  www.catnmsplan.com/timeline

- Industry Member Release Rollout – Pre-Production Presentation

  www.catnmsplan.com/sites/default/files/2022-04/04.21.22-Full_CAIS_Industry_Member_Rollout.pdf

- *Full CAIS 101* (March 1, 2022)

  www.catnmsplan.com/events/full-cais-101-march-1-2022

Regulation Best Interest: Lessons Learned
Tuesday, May 17, 2022
3:00 p.m. – 4:00 p.m.

Join FINRA staff and industry panelists as they discuss lessons learned from implementing Reg BI. Panelists share what worked, conflicts that have been identified, and examination experiences and expectations.

Moderator:

James Wrona
Vice President & Associate General Counsel, Regulatory
FINRA Office of General Counsel

Panelists:

Evan Charkes
Managing Director and Associate General Counsel
Bank of America

Nicole McCafferty
Senior Director, National Cause and Financial Crimes Detection Programs
FINRA Member Supervision

Linde Murphy
Chief Compliance Officer
M.E. Allison & Co., Inc.

Emily Westerberg Russell
Chief Counsel, Division of Trading and Markets
U.S. Securities and Exchange Commission (SEC)

Regulation Best Interest: Lessons Learned Panelists Bios:

Moderator:

James S. Wrona is Vice President and Associate General Counsel for FINRA in Washington, DC. In this role, he is responsible for various policy initiatives, rule changes and litigation regarding the securities industry. Mr. Wrona formerly was associated with the law firm of K&L Gates LLP, where his practice focused on complex federal litigation. He also previously served as a federal law clerk for the Honorable A. Andrew Hauk of the United States District Court for the Central District of California (Los Angeles). Mr. Wrona is a frequent speaker at securities and litigation conferences and author of numerous law review articles, including *The Best of Both Worlds: A Fact-Based Analysis of the Legal Obligations of Investment Advisers and Broker-Dealers and a Framework for Enhanced Investor Protection*, 68 Bus. Law. 1 (Nov. 2012); *The Securities Industry and the Internet: A Suitable Match?*, 2001 Colum. Bus. L. Rev. 601 (2001).

Panelists:

Evan Charkes is Managing Director and Associate General Counsel for Bank of America, and supports the US Merrill Lynch Wealth Management business, including as chief counsel to the firm's Private Wealth Management advisors. Mr. Charkes has spent a significant portion of his career supporting wealth management businesses, including at Citi, where he was a Managing Director and Deputy General Counsel for its Global Wealth Management business. Mr. Charkes started his career as a litigation associate in private practice in New York City. With respect to participating in industry organizations, Mr. Charkes has served on FINRA's National Adjudicatory Council and is a former member of the FINRA Compliance Advisory Committee and FINRA International Committee. Mr. Charkes also formerly served as the co-chair of the SIFMA Compliance and Regulatory Policy Committee and SIFMA Self-Regulation and Supervisory Practices Committee and has been a frequent speaker at the SIFMA Compliance & Legal Society annual seminar. Mr. Charkes also chaired the Insured Retirement Institute's Securities Committee and has contributed numerous articles to the *New York Law Journal* and *Wall Street Lawyer* regarding securities law. Mr. Charkes is a member of the Board of Directors of the Pro Bono Partnership, a non-profit organization that provides legal services to nonprofit organizations in Connecticut, New Jersey, and New York. Mr. Charkes is a graduate of Georgetown University Law Center and Columbia College.

Nicole McCafferty is Senior Director in FINRA's National Cause and Financial Crimes Detection Programs where she provides critical leadership and strategic support to the Executive Vice President to effectively achieve the goals and priorities of the department. In her prior role as Examination Director in FINRA's Member Supervision Department under the Retail firm grouping, she was responsible for managing a team of examination managers and examiners that executed examinations of member firms who primarily conducted business with retail investors. Ms. McCafferty has also held positions as an Examination Manager and Examiner in her 13-year tenure. Ms. McCafferty began her career at the NYSE as a Sales Practice Examiner in 2005 (merging into FINRA in 2007), joined Morgan Stanley's Internal Audit Department in 2009 and then rejoined FINRA in late 2012. She received her B.S. in Finance and Management from Manhattan College.

Linde Murphy currently serves as President and CCO at M.E. Allison & Co., Inc., a full-service broker/dealer and Texas registered investment adviser. Founded in 1946, the firm also provides municipalities with advisory and underwriting services. In 2012, Ms. Murphy joined Presidio Financial Services as they began the CMA process to join M.E. Allison & Co., Inc. Ms. Murphy started her career in investments on a trading desk in Chicago in 1999 and has held positions in compliance, sales, business development and management. In addition to the pertinent industry licenses, Ms. Murphy obtained the CRCP™ designation in 2014 after attending the FINRA Institute at Wharton on the FINRA Small Firm scholarship. She currently serves on the FINRA Board of Governors. She previously chaired the FINRA Small Firm Advisory Committee

and served on the District 6 Committee, the FINRA Fixed Income Committee and the FINRA Regulatory Advisory Committee.

Emily Westerberg Russell was named Chief Counsel of the SEC's Division of Trading and Markets in July 2019, after serving as a member of the Office of Chief Counsel for a decade. The Office of Chief Counsel provides legal and policy advice to the Commission on a variety of matters affecting broker-dealers and the operation of the securities markets. Among other things, the Office was responsible for developing and drafting key components of the Commission's recently adopted package of rulemakings and interpretations designed to enhance the quality and transparency of retail investors' relationships with investment advisers and broker-dealers, in particular, Regulation Best Interest. Ms. Russell received the SEC's Jay Manning Award in 2019 in recognition of her commitment to excellence, dedication to fair and honest markets, and tireless pursuit of just and workable regulatory responses to practical business problems. She also was a joint recipient of the Chairman's Award for Excellence for her work on the IA/BD Team, and a joint recipient of the Law and Policy Award for her work on the Dodd-Frank Legislative Response Team. Prior to joining the SEC, she was a Senior Associate in the Financial Institutions Group at WilmerHale, where she advised broker-dealers and other financial institutions regarding compliance with a wide range of securities and banking laws, including anti-money laundering requirements. Ms. Russell received her J.D. from Columbia University School of Law, where she was a James Kent and a Harlan Fiske Stone Scholar, and served as Executive Editor of the *Columbia Journal of Transnational Law*. She earned her B.A., *summa cum laude*, in economics and international relations from Colgate University.

Regulation Best Interest: Lessons Learned

Panelists

- **Moderator**
  - James Wrona, Vice President & Associate General Counsel, Regulatory, FINRA Office of General Counsel
- **Panelists**
  - Evan Charkes, Managing Director and Associate General Counsel, Bank of America
  - Nicole McCafferty, Senior Director, National Cause and Financial Crimes Detection Programs, FINRA Member Supervision
  - Linde Murphy, Chief Compliance Officer, M.E. Allison & Co., Inc.
  - Emily Westerberg Russell, Chief Counsel, Division of Trading and Markets, U.S. Securities and Exchange Commission (SEC)

Regulation Best Interest: Lessons Learned
Tuesday, May 17, 2022
3:00 p.m. – 4:00 p.m.

Resources:

- SEC Staff Bulletin: Standards of Conduct for Broker-Dealers and Investment Advisers Account Recommendations for Retail Investors

  www.sec.gov/tm/iabd-staff-bulletin

- 2022 Report on FINRA's Examination and Risk Monitoring Program (Reg BI and Form CRS Section)

  www.finra.org/rules-guidance/guidance/reports/2022-finras-examination-and-risk-monitoring-program/reg-bi-form-crs

APPENDIX B

UNITED STATES[1]
SECURITIES AND EXCHANGE COMMISSION

OMB APPROVAL	
OMB Number:	3235-0766
Expires:	[Date]
Estimated average burden hours per response:	[xx.xx]

FORM CRS

Sections 3, 10, 15, 15(c)(6), 15(*l*), 17, 23, and 36 of the Securities Exchange Act of 1934 ("Exchange Act") and section 913(f) of Title IX of the Dodd-Frank Act authorize the Commission to require the collection of the information on Form CRS from brokers and dealers. *See* 15 U.S.C. 78c, 78j, 78o, 78o(c)(6), 78o(*l*), 78q, 78w and 78mm. Filing Form CRS is mandatory for every broker or dealer registered with the Commission pursuant to section 15 of the Exchange Act that offers services to a retail investor. *See* 17 CFR 240.17a-14. Intentional misstatements or omissions constitute federal criminal violations (*see* 18 U.S.C. 1001 and 15 U.S.C. 78ff(a)). The Commission may use the information provided in Form CRS to manage its regulatory and examination programs. Form CRS is made publically available.

An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid control number. Any member of the public may direct to the Commission any comments concerning the accuracy of this burden estimate and any suggestions for reducing this burden. This collection of information has been reviewed by the Office of Management and Budget in accordance with the requirements of 44 U.S.C. 3507.

The information contained in the form is part of a system of records subject to the Privacy Act of 1974, as amended. The information may be disclosed as outlined above and in the routine uses listed in the applicable system of records notice, SEC-70, SEC's Division of Trading and Markets Records, published in the Federal Register at 83 FR 6892 (February 15, 2018).

---

[1] This cover page will be included for Form CRS (17 CFR 249.640) only.

[Form ADV, Part 3: Instructions to Form CRS][2]

General Instructions

Under rule 17a-14 under the Securities Exchange Act of 1934 and rule 204-5 under the Investment Advisers Act of 1940, broker-dealers registered under section 15 of the Exchange Act and investment advisers registered under section 203 of the Advisers Act are required to deliver to *retail investors* a *relationship summary* disclosing certain information about the firm.[3] Read all the General Instructions as well as the particular item requirements before preparing or updating the *relationship summary*.

If you do not have any *retail investors* to whom you must deliver a *relationship summary*, you are not required to prepare or file one. See also Advisers Act rule 204-5; Exchange Act rule 17a-14(a).

1. Format.

A. The *relationship summary* must include the required items enumerated below. The items require you to provide specific information.

B. You must respond to each item and must provide responses in the same order as the items appear in these instructions. You may not include disclosure in the *relationship summary* other than disclosure that is required or permitted by these Instructions and the applicable item.

C. You must make a copy of the *relationship summary* available upon request without charge. In paper format, the *relationship summary* for broker-dealers and investment advisers must not exceed two pages. For *dual registrants* that include their brokerage services and investment advisory services in one *relationship summary*, it must not exceed four pages in paper format. *Dual registrants* and *affiliates* that prepare separate *relationship summaries* are limited to two pages for each *relationship summary*. See General Instruction 5. You must use reasonable paper size, font size, and margins. If delivered electronically, the relationship summary must not exceed the equivalent of two pages or four pages in paper format, as applicable.

2. Plain English; Fair Disclosure.

A. The items of the *relationship summary* are designed to promote effective communication between you and *retail investors*. Write your *relationship summary* in plain English, taking into consideration *retail investors*' level of

---

[2] The bracketed text will be included for Form ADV, Part 3 (17 CFR 279.1) only.

[3] Terms that are italicized in these instructions are defined in General Instruction 11.

financial experience. You should include white space and implement other design features to make the *relationship summary* easy to read. The *relationship summary* should be concise and direct. Specifically: (i) use short sentences and paragraphs; (ii) use definite, concrete, everyday words; (iii) use active voice; (iv) avoid legal jargon or highly technical business terms unless you clearly explain them; and (v) avoid multiple negatives. You must write your response to each item as if you are speaking to the *retail investor*, using "you," "us," "our firm," etc.

Note: The SEC's Office of Investor Education and Advocacy has published A Plain English Handbook. You may find the handbook helpful in writing your *relationship summary*. For a copy of this handbook, visit the SEC's website at www.sec.gov/news/extra/handbook.htm.

B. All information in your *relationship summary* must be true and may not omit any material facts necessary in order to make the disclosures required by these Instructions and the applicable Item, in light of the circumstances under which they were made, not misleading. If a required disclosure or conversation starter is inapplicable to your business or specific wording required by these Instructions is inaccurate, you may omit or modify that disclosure or conversation starter.

C. Responses must be factual and provide balanced descriptions to help *retail investors* evaluate your services. For example, you may not include exaggerated or unsubstantiated claims, vague and imprecise "boilerplate" explanations, or disproportionate emphasis on possible investments or activities that are not offered to *retail investors*.

D. Broker-dealers and investment advisers have disclosure and reporting obligations under state and federal laws, including, but not limited to, obligations under the Exchange Act, the Advisers Act, and the respective rules thereunder. Broker-dealers are also subject to disclosure obligations under the rules of self-regulatory organizations. Delivery of the *relationship summary* will not necessarily satisfy the additional requirements that you have under the federal securities laws and regulations or other laws or regulations.

3. Electronic And Graphical Formats.

A. You are encouraged to use charts, graphs, tables, and other graphics or text features in order to respond to the required disclosures. You are also encouraged to use text features, text colors, and graphical cues, such as dual-column charts, to compare services, account characteristics, investments, fees, and conflicts of interest. For a *relationship summary* that is posted on your website or otherwise provided electronically, we encourage online tools that populate information in comparison boxes based on investor selections. You also may include: (i) a means of facilitating access to video or audio messages, or other forms of information (whether by hyperlink, website address, Quick Response Code ("QR code"), or other equivalent methods or technologies); (ii) mouse-over windows;

(iii) pop-up boxes; (iv) chat functionality; (v) fee calculators; or (vi) other forms of electronic media, communications, or tools designed to enhance a *retail investor's* understanding of the material in the *relationship summary*.

B. In a *relationship summary* that is posted on your website or otherwise provided electronically, you must provide a means of facilitating access to any information that is referenced in the *relationship summary* if the information is available online, including, for example, hyperlinks to fee schedules, conflicts disclosures, the firm's narrative brochure required by Part 2A of Form ADV, or other regulatory disclosures. In a *relationship summary* that is delivered in paper format, you may include URL addresses, QR codes, or other means of facilitating access to such information.

C. Explanatory or supplemental information included in the *relationship summary* pursuant to General Instructions 3.A. or 3.B.: (i) must be responsive to and meet the requirements in these instructions for the particular Item in which the information is placed; and (ii) may not, because of the nature, quantity, or manner of presentation, obscure or impede understanding of the information that must be included. When using interactive graphics or tools, you may include instructions on their use and interpretation.

4. <u>Formatting For Conversation Starters, Additional Information, and Standard of Conduct.</u>

A. For the "conversation starters" required by Items 2, 3, 4, and 5 below, you must use text features to make the conversation starters more noticeable and prominent in relation to other discussion text, for example, by: using larger or different font, a text box around the heading or questions; bolded, italicized or underlined text; or lines to offset the questions from the other sections.

B. Investment advisers that provide only automated investment advisory services or broker-dealers that provide services only online without a particular individual with whom a *retail investor* can discuss these conversation starters must include a section or page on their website that answers each of the questions and must provide in the *relationship summary* a means of facilitating access to that section or page. If you provide automated investment advisory or brokerage services but also make a financial professional available to discuss your services with a *retail investor*, a financial professional must be available to discuss these conversation starters with the *retail investor*.

C. For references to additional information regarding services, fees, and conflicts of interest required by Items 2.C., 3.A.(iii), and 3.B.(iv) below, you must use text features to make this information more noticeable and prominent in relation to other discussion text, for example, by: using larger or different font, a text box around the heading or questions, bolded, italicized or underlined text, or lines to offset the information from the other sections. A *relationship summary* provided

electronically must include a hyperlink, QR code, or other means of facilitating access that leads directly to the relevant additional information.

5. *Dual Registrants*, *Affiliates*, and Additional Services.

A. If you are a *dual registrant*, you are encouraged to prepare a single *relationship summary* discussing both your brokerage and investment advisory services. Alternatively, you may prepare two separate *relationship summaries* for brokerage services and investment advisory services. Whether you prepare a single *relationship summary* or two, you must present the brokerage and investment advisory information with equal prominence and in a manner that clearly distinguishes and facilitates comparison of the two types of services. If you prepare two separate *relationship summaries*, you must reference and provide a means of facilitating access to the other, and you must deliver to each *retail investor* both *relationship summaries* with equal prominence and at the same time, without regard to whether the particular *retail investor* qualifies for those retail services or accounts.

B. If you are a broker-dealer or investment adviser and your *affiliate* also provides brokerage or investment advisory services to *retail investors*, you may prepare a single *relationship summary* discussing the services you and your *affiliate* provide. Alternatively, you may prepare separate *relationship summaries* for your services and your *affiliate's* services.

(i) Whether you prepare a single *relationship summary* or separate *relationship summaries*, you must design them in a manner that presents the brokerage and investment advisory information with equal prominence and clearly distinguishes and facilitates comparison of the two types of services.

(ii) If you prepare separate *relationship summaries*:

a. If a *dually licensed financial professional* provides brokerage and investment advisory services on behalf of you and your *affiliate*, you must deliver to each *retail investor* both your and your *affiliate's relationship summaries* with equal prominence and at the same time, without regard to whether the particular *retail investor* qualifies for those retail services or accounts. Each of the *relationship summaries* must reference and provide a means of facilitating access to the other.

b. If General Instruction 5.B.(ii)(a) does not apply, you may choose whether or not to reference and provide a means of facilitating access to your *affiliate's relationship summary* and whether or not to deliver your and your *affiliate's relationship summaries* to each *retail investor* with equal prominence and at the same time.

C. You may acknowledge other financial services that you provide in addition to your services as a broker-dealer or investment adviser registered with the SEC, such as insurance, banking, or retirement services, or investment advice pursuant to state registration or licensing. You may include references and means of facilitating access to additional information about those services. Information not pertaining to brokerage or investment advisory services may not, because of the nature, quantity, or manner of presentation, obscure or impede understanding of the information that must be included. See also General Instruction 3.C.

6. Preserving Records.

A. You must maintain records in accordance with Advisers Act rule 204-2(a)(14)(i) and/or Exchange Act rule 17a-4(e)(10), as applicable.

7. Initial Filing and Delivery; Transition Provisions.

A. **Initial filing.**

(i) If you are an investment adviser and are required to deliver a *relationship summary* to a *retail investor*, you must file Form ADV, Part 3 (Form CRS) electronically with the Investment Adviser Registration Depository (IARD). If you are a registered broker-dealer and are required to deliver a *relationship summary* to a *retail investor*, you must file Form CRS electronically through the Central Registration Depository ("Web CRD®") operated by the Financial Industry Regulatory Authority, Inc. (FINRA). If you are a *dual registrant* and are required to deliver a *relationship summary* to one or more *retail investor* clients or customers of both your investment advisory and brokerage businesses, you must file using IARD and Web CRD®. You must file Form CRS using a text-searchable format with machine-readable headings.

(ii) Information for investment advisers on how to file with IARD is available on the SEC's website at www.sec.gov/iard. Information for broker-dealers on how to file through Web CRD® is available on FINRA's website at http://www.finra.org/industry/web-crd/web-crd-system-links.

B. **Initial delivery.**

(i) *Investment Advisers*: If you are an investment adviser, you must deliver a *relationship summary* to each *retail investor* before or at the time you enter into an investment advisory contract with the *retail investor*. You must deliver the *relationship summary* even if your agreement with the *retail investor* is oral. See Advisers Act rule 204-5(b)(1).

(ii) *Broker-Dealers*: If you are a broker-dealer, you must deliver a *relationship summary* to each *retail investor*, before or at the earliest of: (i) a recommendation of an account type, a securities transaction, or an investment strategy involving securities; (ii) placing an order for the *retail*

investor; or (iii) the opening of a brokerage account for the *retail investor*. See Exchange Act rule 17a-14(c)(1).

(iii) *Dual Registrants*: A *dual registrant* must deliver the *relationship summary* at the earlier of the timing requirements in General Instruction 7.B.(i) or (ii).

C. **Transition provisions for initial filing and delivery after the effective date of the new Form CRS requirements.**

(i) *Filings for Investment Advisers*

a. If you are already registered or have an application for registration pending with the SEC as an investment adviser before June 30, 2020 you must electronically file, in accordance with Instruction 7.A. above, your initial *relationship summary* beginning on May 1, 2020 and by no later than June 30, 2020 either as: (1) an other-than-annual amendment or (2) part of your initial application or *annual updating amendment*. See Advisers Act rules 203-1 and 204-1.

b. If you file an application for registration with the SEC as an investment adviser on or after June 30, 2020, the Commission will not accept any initial application that does not include a *relationship summary*. See Advisers Act rule 203-1.

(ii) *Filings for Broker-Dealers*

a. If you are already registered with the SEC as a broker-dealer before June 30, 2020, you must electronically file, in accordance with Instruction 7.A. above, your initial *relationship summary* beginning on May 1, 2020 and by no later than June 30, 2020. See Exchange Act rule 17a-14.

b. If you file an application for registration or have an application pending with the SEC as a broker-dealer on or after June 30, 2020, you must file your *relationship summary* by no later than the date that your registration becomes effective. See Exchange Act rule 17a-14.

(iii) *Delivery to New and Prospective Clients and Customers:* As of the date by which you are first required to electronically file your *relationship summary* with the SEC, you must begin to deliver your *relationship summary* to new and prospective clients and customers who are *retail investors* as required by Instruction 7.B. See Advisers Act rule 204-5 and Exchange Act rule 17a-14.

(iv) *Delivery to Existing Clients and Customers:* Within 30 days after the date by which you are first required to electronically file your *relationship*

summary with the SEC, you must deliver your *relationship summary* to each of your existing clients and customers who are *retail investors*. See Advisers Act rule 204-5 and Exchange Act rule 17a-14.

8. Updating the *Relationship Summary* and Filing Amendments.

A. You must update your *relationship summary* and file it in accordance with Instruction 7.A. above within 30 days whenever any information in the *relationship summary* becomes materially inaccurate. The filing must include an exhibit highlighting changes required by Instruction 8.C. below.

B. You must communicate any changes in the updated *relationship summary* to *retail investors* who are existing clients or customers within 60 days after the updates are required to be made and without charge. You can make the communication by delivering the amended *relationship summary* or by communicating the information through another disclosure that is delivered to the *retail investor*.

C. Each amended *relationship summary* that is delivered to a *retail investor* who is an existing client or customer must highlight the most recent changes by, for example, marking the revised text or including a summary of material changes. The additional disclosure showing revised text or summarizing the material changes must be attached as an exhibit to the unmarked amended *relationship summary*.

9. Additional Delivery Requirements to Existing Clients and Customers.

A. You must deliver the most recent *relationship summary* to a *retail investor* who is an existing client or customer before or at the time you: (i) open a new account that is different from the *retail investor's* existing account(s); (ii) recommend that the *retail investor* roll over assets from a retirement account into a new or existing account or investment; or (iii) recommend or provide a new brokerage or investment advisory service or investment that does not necessarily involve the opening of a new account and would not be held in an existing account, for example, the first-time purchase of a direct-sold mutual fund or insurance product that is a security through a "check and application" process, *i.e.*, not held directly within an account.

B. You also must deliver the *relationship summary* to a *retail investor* within 30 days upon the *retail investor's* request.

10. Electronic Posting and Manner of Delivery.

A. You must post the current version of the *relationship summary* prominently on your public website, if you have one, in a location and format that is easily accessible for *retail investors*.

B. You may deliver the *relationship summary* electronically, including updates, consistent with SEC guidance regarding electronic delivery, in particular Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information, which you can find at www.sec.gov/rules/concept/33-7288.txt. You may deliver the *relationship summary* to new or prospective clients or customers in a manner that is consistent with how the *retail investor* requested information about you or your financial professional consistent with SEC guidance, in particular Form CRS Relationship Summary; Amendments to Form ADV, which you can find at https://www.sec.gov/rules/final/2019/34-86032.pdf.

C. If the *relationship summary* is delivered electronically, it must be presented prominently in the electronic medium, for example, as a direct link or in the body of an email or message, and must be easily accessible for *retail investor*s.

D. If the *relationship summary* is delivered in paper format as part of a package of documents, you must ensure that the *relationship summary* is the first among any documents that are delivered at that time.

11. Definitions.

For purposes of Form CRS and these Instructions, the following terms have the meanings ascribed to them below:

A. **Affiliate:** Any persons directly or indirectly controlling or controlled by you or under common control with you.

B. **Dually licensed financial professional:** A natural person who is both an associated person of a broker-dealer registered under section 15 of the Exchange Act, as defined in section 3(a)(18) of the Exchange Act, and a supervised person of an investment adviser registered under section 203 of the Advisers Act, as defined in section 202(a)(25) of the Advisers Act.

C. **Dual registrant:** A firm that is dually registered as a broker-dealer under section 15 of the Exchange Act and an investment adviser under section 203 of the Advisers Act and offers services to *retail investors* as both a broker-dealer and an investment adviser. For example, if you are dually registered and offer investment advisory services to *retail investors*, but offer brokerage services only to institutional investors, you are not a *dual registrant* for purposes of Form CRS and these Instructions.

D. **Relationship summary:** A written disclosure statement prepared in accordance with these Instructions that you must provide to *retail investors*. See Advisers Act rule 204-5; Exchange Act rule 17a-14; Form CRS.

E. **Retail investor:** A natural person, or the legal representative of such natural person, who seeks to receive or receives services primarily for personal, family or household purposes.

Item Instructions

Item 1. Introduction

Include the date prominently at the beginning of the *relationship summary* (*e.g.*, in the header or footer of the first page or in a similar location for a *relationship summary* provided electronically). Briefly discuss the following information in an introduction:

A. State your name and whether you are registered with the Securities and Exchange Commission as a broker-dealer, investment adviser, or both. Also indicate that brokerage and investment advisory services and fees differ and that it is important for the *retail investor* to understand the differences. You may also include a reference to FINRA or Securities Investor Protection Corporation membership in a manner consistent with other rules or regulations (*e.g.*, FINRA rule 2210).

B. State that free and simple tools are available to research firms and financial professionals at Investor.gov/CRS, which also provides educational materials about broker-dealers, investment advisers, and investing.

Item 2. Relationships and Services

A. Use the heading: "What investment services and advice can you provide me?"

B. **Description of Services:** State that you offer brokerage services, investment advisory services, or both, to *retail investors*, and summarize the principal services, accounts, or investments you make available to *retail investors*, and any material limitations on such services. For broker-dealers, state the particular types of principal brokerage services you offer to *retail investors*, including buying and selling securities, and whether or not you offer recommendations to *retail investors*. For investment advisers, state the particular types of principal investment advisory services you offer to *retail investors*, including, for example, financial planning and wrap fee programs.

In your description you must address the following:

(i) *Monitoring:* Explain whether or not you monitor *retail investors'* investments, including the frequency and any material limitations. If so, indicate whether or not the services described in response to this Item 2.B.(i) are offered as part of your standard services.

(ii) *Investment Authority*: For investment advisers that accept discretionary authority, describe those services and any material limitations on that authority. Any such summary must include the specific circumstances that would trigger this authority and any material limitations on that authority (*e.g.*, length of time). For investment advisers that offer non-discretionary services and broker-dealers, explain that the *retail investor* makes the ultimate decision regarding the purchase or sale of investments.

Broker-dealers may, but are not required to state whether you accept limited discretionary authority.

Note: If you are a broker-dealer offering recommendations, you should consider the applicability of the Investment Advisers Act of 1940, consistent with SEC guidance.

(iii) *Limited Investment Offerings*: Explain whether or not you make available or offer advice only with respect to proprietary products, or a limited menu of products or types of investments, and if so, describe these limitations.

(iv) *Account Minimums and Other Requirements*: Explain whether or not you have any requirements for *retail investors* to open or maintain an account or establish a relationship, such as minimum account size or investment amount.

C. **Additional Information:** Include specific references to more detailed information about your services that, at a minimum, include the same or equivalent information to that required by the Form ADV, Part 2A brochure (Items 4 and 7 of Part 2A or Items 4.A. and 5 of Part 2A Appendix 1) and Regulation Best Interest, as applicable. If you are a broker-dealer that does not provide recommendations subject to Regulation Best Interest, to the extent you prepare more detailed information about your services, you must include specific references to such information. You may include hyperlinks, mouse-over windows, or other means of facilitating access to this additional information and to any additional examples or explanations of such services.

D. **Conversation Starters:** Include the following additional questions for a *retail investor* to ask a financial professional and start a conversation about relationships and services:

(i) If you are a broker-dealer and not a *dual registrant*, include: "Given my financial situation, should I choose a brokerage service? Why or why not?"

(ii) If you are an investment adviser and not a *dual registrant*, include: "Given my financial situation, should I choose an investment advisory service? Why or why not?"

(iii) If you are a *dual registrant*, include: "Given my financial situation, should I choose an investment advisory service? Should I choose a brokerage service? Should I choose both types of services? Why or why not?"

(iv) "How will you choose investments to recommend to me?"

(v) "What is your relevant experience, including your licenses, education and other qualifications? What do these qualifications mean?"

Item 3. **Fees, Costs, Conflicts, and Standard of Conduct**

A. Use the heading: "What fees will I pay?"

(i) *Description of Principal Fees and Costs*: Summarize the principal fees and costs that *retail investors* will incur for your brokerage or investment advisory services, including how frequently they are assessed and the conflicts of interest they create.

a. Broker-dealers must describe their transaction-based fees. With respect to addressing conflicts of interest, a broker-dealer could, for example, include a statement that a *retail investor* would be charged more when there are more trades in his or her account, and that the firm may therefore have an incentive to encourage a *retail investor* to trade often.

b. Investment advisers must describe their ongoing asset-based fees, fixed fees, wrap fee program fees, or other direct fee arrangement. The principal fees for investment advisory services should align with the type of fee(s) that you report in response to Form ADV Part 1A, Item 5.E.

(1) Include information about each type of fee you report in Form ADV that is responsive to this Item 3.A. Investment advisers with wrap fee program fees are encouraged to explain that asset-based fees associated with the wrap fee program will include most transaction costs and fees to a broker-dealer or bank that has custody of these assets, and therefore are higher than a typical asset-based advisory fee.

(2) With respect to addressing conflicts of interest, an investment adviser that charges an asset-based fee could, for example, include a statement that the more assets there are in a *retail investor's* advisory account, the more a *retail investor* will pay in fees, and the firm may therefore have an incentive to encourage the *retail investor* to increase the assets in his or her account.

Note: If you receive compensation in connection with the purchase or sale of securities, you should carefully consider the applicability of the broker-dealer registration requirements of the Securities Exchange Act of 1934 and any applicable state securities statutes.

(ii) *Description of Other Fees and Costs*: Describe other fees and costs related to your brokerage or investment advisory services and investments in addition to the firm's principal fees and costs disclosed in Item 3.A.(i) that the *retail investor* will pay directly or indirectly. List examples of the

categories of the most common fees and costs applicable to your *retail investors* (*e.g.*, custodian fees, account maintenance fees, fees related to mutual funds and variable annuities, and other transactional fees and product-level fees).

(iii) *Additional Information*: State "You will pay fees and costs whether you make or lose money on your investments. Fees and costs will reduce any amount of money you make on your investments over time. Please make sure you understand what fees and costs you are paying." You must include specific references to more detailed information about your fees and costs that, at a minimum, include the same or equivalent information to that required by the Form ADV, Part 2A brochure (specifically Items 5.A., B., C., and D.) and Regulation Best Interest, as applicable. If you are a broker-dealer that does not provide recommendations subject to Regulation Best Interest, to the extent you prepare more detailed information about your fees and costs, you must include specific references to such information. You may include hyperlinks, mouse-over windows, or other means of facilitating access to this additional information and to any additional examples or explanations of such fees and costs included in response to Item 3.A.(i) or (ii).

(iv) *Conversation Starter*: Include the following question for a *retail investor* to ask a financial professional and start a conversation about the impact of fees and costs on investments: "Help me understand how these fees and costs might affect my investments. If I give you $10,000 to invest, how much will go to fees and costs, and how much will be invested for me?"

B. If you are a broker-dealer, use the heading: "What are your legal obligations to me when providing recommendations? How else does your firm make money and what conflicts of interest do you have?" If you are an investment adviser, use the heading: "What are your legal obligations to me when acting as my investment adviser? How else does your firm make money and what conflicts of interest do you have?" If you are a *dual registrant* that prepares a single *relationship summary*, use the heading: "What are your legal obligations to me when providing recommendations as my broker-dealer or when acting as my investment adviser? How else does your firm make money and what conflicts of interest do you have?"

(i) *Standard of Conduct*.

a. If you are a broker-dealer that provides recommendations subject to Regulation Best Interest, include (emphasis required): "*When we provide you with a recommendation*, we have to act in your best interest and not put our interest ahead of yours. At the same time, the way we make money creates some conflicts with your interests. You should understand and ask us about these conflicts because

they can affect the recommendations we provide you. Here are some examples to help you understand what this means." If you are a broker-dealer that does not provide recommendations subject to Regulation Best Interest, include (emphasis required): "We *do not* provide recommendations. The way we make money creates some conflicts with your interests. You should understand and ask us about these conflicts because they can affect the services we provide you. Here are some examples to help you understand what this means."

b. If you are an investment adviser, include (emphasis required): "*When we act as your investment adviser*, we have to act in your best interest and not put our interest ahead of yours. At the same time, the way we make money creates some conflicts with your interests. You should understand and ask us about these conflicts because they can affect the investment advice we provide you. Here are some examples to help you understand what this means."

c. If you are a *dual registrant* that prepares a single *relationship summary* and you provide recommendations subject to Regulation Best Interest as a broker-dealer, include (emphasis required): "*When we provide you with a recommendation as your broker-dealer or act as your investment adviser*, we have to act in your best interest and not put our interest ahead of yours. At the same time, the way we make money creates some conflicts with your interests. You should understand and ask us about these conflicts because they can affect the recommendations and investment advice we provide you. Here are some examples to help you understand what this means." If you are a *dual registrant* that prepares a single *relationship summary* and you do not provide recommendations subject to Regulation Best Interest as a broker-dealer, include (emphasis required): "We *do not* provide recommendations as your broker-dealer. *When we act as your investment adviser*, we have to act in your best interest and not put our interests ahead of yours. At the same time, the way we make money creates some conflicts with your interest. You should understand and ask us about these conflicts because they can affect the services and investment advice we provide you. Here are some examples to help you understand what this means." If you are a *dual registrant* that prepares two separate *relationship summaries*, follow the instructions for broker-dealers and investment advisers in Items 3.B., 3.B.(i).a., and 3.B.(i).b.

(ii) *Examples of Ways You Make Money and Conflicts of Interest*: If applicable to you, summarize the following other ways in which you and your *affiliates* make money from brokerage or investment advisory

services and investments you provide to *retail investors*. If none of these conflicts applies to you, summarize at least one other material conflict of interest that affects *retail investors*. Explain the incentives created by each of these examples.

a. Proprietary Products: Investments that are issued, sponsored, or managed by you or your *affiliates*.

b. Third-Party Payments: Compensation you receive from third parties when you recommend or sell certain investments.

c. Revenue Sharing: Investments where the manager or sponsor of those investments or another third party (such as an intermediary) shares with you revenue it earns on those investments.

d. Principal Trading: Investments you buy from a *retail investor*, and/or investments you sell to a *retail investor*, for or from your own accounts, respectively.

(iii) *Conversation Starter*: Include the following question for a *retail investor* to ask a financial professional and start a conversation about conflicts of interest: "How might your conflicts of interest affect me, and how will you address them?"

(iv) *Additional Information*: You must include specific references to more detailed information about your conflicts of interest that, at a minimum, include the same or equivalent information to that required by the Form ADV, Part 2A brochure and Regulation Best Interest, as applicable. If you are a broker-dealer that does not provide recommendations subject to Regulation Best Interest, to the extent you prepare more detailed information about your conflicts, you must include specific references to such information. You may include hyperlinks, mouse-over windows, or other means of facilitating access to this additional information and to any additional examples or explanations of such conflicts of interest.

C. Use the heading: "How do your financial professionals make money?"

(i) *Description of How Financial Professionals Make Money*: Summarize how your financial professionals are compensated, including cash and non-cash compensation, and the conflicts of interest those payments create.

(ii) *Required Topics in the Description*: Include, to the extent applicable, whether your financial professionals are compensated based on factors such as: the amount of client assets they service; the time and complexity required to meet a client's needs; the product sold (*i.e.*, differential compensation); product sales commissions; or revenue the firm earns from the financial professional's advisory services or recommendations.

Item 4. Disciplinary History

A. Use the heading: "Do you or your financial professionals have legal or disciplinary history?"

B. State "Yes" if you or any of your financial professionals currently disclose, or are required to disclose, the following information:

(i) Disciplinary information in your Form ADV (Item 11 of Part 1A or Item 9 of Part 2A).

(ii) Legal or disciplinary history in your Form BD (Items 11 A–K) (except to the extent such information is not released to BrokerCheck, pursuant to FINRA Rule 8312).

(iii) Disclosures for any of your financial professionals in Items 14 A–M on Form U4 (Uniform Application for Securities Industry Registration or Transfer), or in Items 7A or 7C–F of Form U5 (Uniform Termination Notice for Securities Industry Registration), or on Form U6 (Uniform Disciplinary Action Reporting Form) (except to the extent such information is not released to BrokerCheck, pursuant to FINRA Rule 8312).

C. State "No" if neither you nor any of your financial professionals currently discloses, or is required to disclose, the information listed in Item 4.B.

D. Regardless of your response to Item 4.B, you must:

(i) *Search Tool*: Direct the *retail investor* to visit Investor.gov/CRS for a free and simple search tool to research you and your financial professionals.

(ii) *Conversation Starter*: Include the following questions for a *retail investor* to ask a financial professional and start a conversation about the financial professional's disciplinary history: "As a financial professional, do you have any disciplinary history? For what type of conduct?"

Item 5. Additional Information

A. State where the *retail investor* can find additional information about your brokerage or investment advisory services and request a copy of the *relationship summary*. This information should be disclosed prominently at the end of the *relationship summary*.

B. Include a telephone number where *retail investors* can request up-to-date information and request a copy of the *relationship summary*.

C. **Conversation Starter:** Include the following questions for a *retail investor* to ask a financial professional and start a conversation about the contacts and complaints: "Who is my primary contact person? Is he or she a representative of an investment adviser or a broker-dealer? Who can I talk to if I have concerns about how this person is treating me?"

Electronic Code of Federal Regulations

We invite you to try out our new beta eCFR site at https://ecfr.federalregister.gov. We have made big changes to make the eCFR easier to use. Be sure to leave feedback using the Feedback button on the bottom right of each page!

e-CFR data is current as of April 5, 2021

Title 17: Commodity and Securities Exchanges
PART 240—GENERAL RULES AND REGULATIONS, SECURITIES EXCHANGE ACT OF 1934

§240.15l-1 Regulation best interest.

(a) *Best interest obligation.* (1) A broker, dealer, or a natural person who is an associated person of a broker or dealer, when making a recommendation of any securities transaction or investment strategy involving securities (including account recommendations) to a retail customer, shall act in the best interest of the retail customer at the time the recommendation is made, without placing the financial or other interest of the broker, dealer, or natural person who is an associated person of a broker or dealer making the recommendation ahead of the interest of the retail customer.

(2) The best interest obligation in paragraph (a)(1) of this section shall be satisfied if:

(i) *Disclosure obligation.* The broker, dealer, or natural person who is an associated person of a broker or dealer, prior to or at the time of the recommendation, provides the retail customer, in writing, full and fair disclosure of:

(A) All material facts relating to the scope and terms of the relationship with the retail customer, including:

(*1*) That the broker, dealer, or such natural person is acting as a broker, dealer, or an associated person of a broker or dealer with respect to the recommendation;

(*2*) The material fees and costs that apply to the retail customer's transactions, holdings, and accounts; and

(*3*) The type and scope of services provided to the retail customer, including any material limitations on the securities or investment strategies involving securities that may be recommended to the retail customer; and

(B) All material facts relating to conflicts of interest that are associated with the recommendation.

(ii) *Care obligation.* The broker, dealer, or natural person who is an associated person of a broker or dealer, in making the recommendation, exercises reasonable diligence, care, and skill to:

(A) Understand the potential risks, rewards, and costs associated with the recommendation, and have a reasonable basis to believe that the recommendation could be in the best interest of at least some retail customers;

(B) Have a reasonable basis to believe that the recommendation is 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 and does not place the financial or other interest of the broker, dealer, or such natural person ahead of the interest of the retail customer;

(C) Have 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 and does not place the financial or other interest of the broker, dealer, or such natural person making the series of recommendations ahead of the interest of the retail customer.

(iii) *Conflict of interest obligation.* The broker or dealer establishes, maintains, and enforces written policies and procedures reasonably designed to:

(A) Identify and at a minimum disclose, in accordance with paragraph (a)(2)(i) of this section, or eliminate, all conflicts of interest associated with such recommendations;

(B) Identify and mitigate any conflicts of interest associated with such recommendations that create an incentive for a natural person who is an associated person of a broker or dealer to place the interest of the broker, dealer, or such natural person ahead of the interest of the retail customer;

(C)(*1*) Identify and disclose any material limitations placed on the securities or investment strategies involving securities that may be recommended to a retail customer and any conflicts of interest associated with such limitations, in accordance with subparagraph (a)(2)(i), and

(*2*) Prevent such limitations and associated conflicts of interest from causing the broker, dealer, or a natural person who is an associated person of the broker or dealer to make recommendations that place the interest of the broker, dealer, or such natural person ahead of the interest of the retail customer; and

(D) Identify and eliminate any sales contests, sales quotas, bonuses, and non-cash compensation that are based on the sales of specific securities or specific types of securities within a limited period of time.

(iv) *Compliance obligation.* In addition to the policies and procedures required by paragraph (a)(2)(iii) of this section, the broker or dealer establishes, maintains, and enforces written policies and procedures reasonably designed to achieve compliance with Regulation Best Interest.

(b) *Definitions.* Unless otherwise provided, all terms used in this rule shall have the same meaning as in the Securities Exchange Act of 1934. In addition, the following definitions shall apply for purposes of this section:

(1) *Retail customer* means a natural person, or the legal representative of such natural person, who:

(i) Receives a recommendation of any securities transaction or investment strategy involving securities from a broker, dealer, or a natural person who is an associated person of a broker or dealer; and

(ii) Uses the recommendation primarily for personal, family, or household purposes.

(2) *Retail customer investment profile* includes, but is not limited to, the retail customer's age, other investments, financial situation and needs, tax status, investment objectives, investment experience, investment time horizon, liquidity needs, risk tolerance, and any other information the retail customer may disclose to the broker, dealer, or a natural person who is an associated person of a broker or dealer in connection with a recommendation.

(3) *Conflict of interest* means an interest that might incline a broker, dealer, or a natural person who is an associated person of a broker or dealer —consciously or unconsciously—to make a recommendation that is not disinterested.

[84 FR 33491, July 12, 2019]

Need assistance?

Home

gpo.gov

govinfo.gov

Browse / Search Previous

e-CFR Navigation Aids

Browse

Simple Search

Advanced Search

— Boolean

— Proximity

Search History

Search Tips

Corrections

Latest Updates

User Info

FAQs

Agency List

Incorporation By Reference

Related Resources

The Code of Federal Regulations (CFR) annual edition is the codification of the general and permanent rules published in the Federal Register by the departments and agencies of the Federal Government produced by the Office of the Federal Register (OFR) and the Government Publishing Office.

Download the Code of Federal Regulations in XML.

Download the Electronic Code of Federal Regulations in XML.

Monthly Title and Part user viewing data for the e-CFR is available for download in CSV format.

Parallel Table of Authorities and Rules for the Code of Federal Regulations and the United States Code
Text | PDF

Find, review, and submit comments on Federal rules that are open for comment and published in the Federal Register using Regulations.gov.

Purchase individual CFR titles from the U.S. Government Online Bookstore.

Find issues of the CFR (including issues prior to 1996) at a local Federal depository library.

[A2]

2022 Annual Conference

May 16 –18 | Washington, DC | Hybrid Event

Underwriting Trends
Tuesday, May 17, 2022
3:00 p.m. – 4:00 p.m.

During this session, FINRA staff and industry practitioners discuss underwriting trends and observations. Panelists discuss what you need to know about equality, debt and alternative offerings, syndicate practices and developments in the regulatory environment.

Moderator:

Paul Mathews
Vice President and Director, Corporate Financing
FINRA Corporate Financing

Panelists:

Gabriela Aguero
Director, Public Offerings
FINRA Corporate Financing

Leslie Gardner
Managing Director & Associate General Counsel
J.P. Morgan

Jeffrey Whyte
General Counsel, Investment Banking, Managing Director
Jefferies LLC

Underwriting Trends Panelists Bios:

Moderator:

Paul Mathews is Vice President and Director of FINRA's Corporate Financing Department. The Department administers FINRA rules that regulate public and private securities offerings. The Department's regulatory functions include reviewing offerings for compliance with FINRA and SEC rules, conducting investigations, and providing interpretive assistance and policy support. Mr. Mathews has been active in numerous FINRA regulatory initiatives addressing broker-dealer obligations in public and private offerings, including the development of new rules, modernization of existing requirements and the publication of guidance on various issues. Mr. Mathews is a staff liaison to FINRA's Corporate Financing Committee and serves on various FINRA task forces and internal committees. He was previously Associate Director and Enforcement Liaison for the Department, in which capacity he managed investigations staff and targeted a variety of problems through sweeps and examinations. During his career with FINRA he has worked on international regulatory initiatives, examination procedures and systems, new product regulation, arbitrations, statutory disqualifications and licensing/registration. He holds a BA in Economics from the University of Virginia, an MBA from Virginia Tech, and a regulatory professional designation from Wharton.

Panelists:

Gabriela Aguero is Director in FINRA's Corporate Financing Department. In her role, she oversees the Public Offering Review (POR) program. The POR group is responsible for the review of a wide array of filings and the interpretation and application of FINRA's rules that regulate underwriting activities and conflicts of interests in public offerings. Ms. Aguero began her career at FINRA when she joined NASD in 2000. She has an MBA from the John's Hopkins Carey Business School in addition to an undergraduate degree in Finance as well as designation as a FINRA Certified Regulatory and Compliance Professional™ (CRCP™) Program at Wharton.

Leslie Gardner is Managing Director and Associate General Counsel in J.P. Morgan's Investment Banking, where she co-heads its Global Banking Practice Group. She manages a large global group of lawyers and legal professionals supporting J.P. Morgan's Capital Markets, Wholesale Lending, M&A Advisory/Conflicts, Investment Banking Coverage, Research and Public Finance origination businesses. Ms. Gardner has held various roles at J.P. Morgan Chase and its heritage entities for the past 30 years. Ms. Gardner is actively involved in J.P. Morgan Civil Liberties pro bono program and is a member of J.P. Morgan's Equity Commitments, Fairness Opinion, Corporate Finance Advisory, Business Control and Reputational Risk Committees. She is a member of FINRA's Corporate Finance Lawyers Committee and previously served as Chair of SIFMA's Capital Markets Committee. Her team of lawyers won IFLR's "Americas In-house Equity Team of the Year" award for four years in recent years and she was named ILFR's "Americas Women in Business Law (In-house)" award recipient in 2014. Prior to joining J.P. Morgan, Ms. Gardner was a corporate lawyer at the New York law firm of Cahill Gordon & Reindel. Ms. Gardner holds a JD from New York University School of Law and a BA from Amherst College and graduated from The Nichols School in Buffalo, New York.

Jeffrey Whyte is Managing Director and General Counsel, Investment Banking at Jefferies LLC. In that role, Mr. Whyte's responsibilities include coverage of all transaction related legal matters relating to equity capital markets, debt capital markets, M&A and restructuring at Jefferies LLC. Mr. Whyte is also a member of the Jefferies' Employee Resource Group, jVets. Mr. Whyte has been with Jefferies since 2008 and prior to that was a partner at White & Case LLP. Mr. Whyte sits on the Board of Trustees, Executive Committee and is the head of the Audit Committee of the Corlears School in New York as well as on the Board of Governors and Finance Committee of the Lake Naomi Club in Pocono Pines, PA. Mr. Whyte earned an

Honorable Discharge from the U.S. Army after serving as a Combat Medical Specialist in the U.S. Army Reserve and Connecticut Army National Guard from 1987-1995. Mr. Whyte holds a B.A., *magna cum laude*, M.A. and J.D. (highest honors) from the University of Connecticut.

Underwriting Trends

Panelists

- **Moderator**
  - Paul Mathews, Vice President and Director, Corporate Financing, FINRA Corporate Financing
- **Panelists**
  - Gabriela Aguero, Director, Public Offerings, FINRA Corporate Financing
  - Leslie Gardner, Managing Director & Associate General Counsel, J.P. Morgan
  - Jeffrey Whyte, General Counsel, Investment Banking, Managing Director, Jefferies LLC

Agenda

01 | Recent Market Volatility

02 | SPAC Underwriting Trends

03 | ESG Trends

04 | Syndicate Settlement Developments

1. Recent Market Volatility and Rising Rates

- Observations – Impacts on Issuers, Investors and IBs
- Recent Trends and Alternatives – What are we Seeing Now?
- FINRA's Public Offering Program – Trends and Observations

2. SPAC Underwriting Trends

- Temporary Slowdown?
- SEC's Proposed New Rules – Potential Impacts and Repercussions
- Alternatives including Direct Listings

3. ESG Trends

- ESG Hot Topics and Trends
- SEC's ESG Proposals – Potential Impacts and Repercussions
- How are Market Participants Reacting?

4. Syndicate Settlement Developments

- Status of FINRA's Proposal to Shorten Settlements to 30 Days
- Small Firm and Large Firm Perspective
- Potential Impacts, Repercussions and Alternatives

Wrap Up

Reference Materials – SPACs

- SEC Proposal Fact Sheet: SPACs, Shell Companies, and Projections
  - *www.sec.gov/files/33-11048-fact-sheet.pdf*
- SEC Special Purpose Acquisition Companies, Shell Companies, and Projections Proposed Rules
  - *www.sec.gov/rules/proposed/2022/33-11048.pdf*
- NYSE Direct Listings Rule Filing
  - *www.nyse.com/publicdocs/nyse/markets/nyse/rule-filings/filings/2022/SR-NYSE-2022-14.pdf*

Reference Materials – ESGs

Enhancement and Standardization of Climate-Related Disclosures

- SEC Proposal Fact Sheet: Enhancement and Standardization of Climate-Related
  - *www.sec.gov/files/33-11042-fact-sheet.pdf*

- SEC The Enhancement and Standardization of Climate-Related Disclosures for Investors Proposed Rules
  - *www.sec.gov/rules/proposed/2022/33-11042.pdf*

Reference Materials – Regulatory Notices

- FINRA *Regulatory Notice 22-06, U.S. Imposes Sanctions on Russian Entities and Individuals* (February 2022)
  - www.finra.org/rules-guidance/notices/22-06

- FINRA *Regulatory Notice 21-40, FINRA Requests Comment on Amendments to Rule 11880 Shortening the Settlement of Syndicate Accounts* (November 2021)
  - www.finra.org/rules-guidance/notices/21-40

Underwriting Trends
Tuesday, May 17, 2022
3:00 p.m. – 4:00 p.m.

Resources:

- FINRA *Regulatory Notice 22-06, U.S. Imposes Sanctions on Russian Entities and Individuals* (February 2022)

  www.finra.org/rules-guidance/notices/22-06

- FINRA *Regulatory Notice 21-40, FINRA Requests Comment on Amendments to Rule 11880 Shortening the Settlement of Syndicate Accounts* (November 2021)

  https://www.finra.org/rules-guidance/notices/21-40

- SEC Proposal Fact Sheet: SPACs, Shell Companies, and Projections

  www.sec.gov/files/33-11048-fact-sheet.pdf

- SEC Special Purpose Acquisition Companies, Shell Companies, and Projections Proposed Rules

  www.sec.gov/rules/proposed/2022/33-11048.pdf

- SEC Proposal Fact Sheet: Enhancement and Standardization of Climate-Related Disclosures

  www.sec.gov/files/33-11042-fact-sheet.pdf

- SEC The Enhancement and Standardization of Climate-Related Disclosures for Investors Proposed Rules

  www.sec.gov/rules/proposed/2022/33-11042.pdf

- NYSE Direct Listings Rule Filing

  www.nyse.com/publicdocs/nyse/markets/nyse/rule-filings/filings/2022/SR-NYSE-2022-14.pdf

Diversity and Inclusion
Tuesday, May 17, 2022
3:00 p.m. – 4:00 p.m.

As the focus on diversity and inclusion in the financial services industry increases, it is important that employers attract, develop and retain the best talent of all backgrounds. This session aims to increase the awareness of diversity and inclusion and explains how to promote and maintain a diverse and inclusive culture within our firms and industry.

Introduction: Robert Cook
President and Chief Executive Officer
FINRA

Speakers: Roel C. Campos
Senior Counsel
Hughes Hubbard & Reed LLP

Audria Pendergrass Lee
Vice President, Talent Acquisition and Chief Diversity Officer
FINRA Human Resources

Diversity and Inclusion Speaker Bios:

Introduction:

Robert W. Cook is President and CEO of FINRA, and Chairman of the FINRA Investor Education Foundation. From 2010 to 2013, Mr. Cook served as the Director of the Division of Trading and Markets of the U.S. Securities and Exchange Commission. Under his direction, the Division's professionals were responsible for regulatory policy and oversight with respect to broker-dealers, securities exchanges and markets, clearing agencies and FINRA. In addition, the Division reviewed and acted on over 2,000 rule filings and new product listings each year from self-regulatory organizations, including the securities exchanges and FINRA, and was responsible for implementing more than 30 major rulemaking actions and studies generated by the Dodd-Frank and JOBS Acts. He also directed the staff's review of equity market structure. Immediately prior to joining FINRA, and before his service at the SEC, Mr. Cook was a partner based in the Washington, DC, office of an international law firm. His practice focused on the regulation of securities markets and market intermediaries, including securities firms, exchanges, alternative trading systems and clearing agencies. During his years of private practice, Mr. Cook worked extensively on broker-dealer regulation, advising large and small firms on a wide range of compliance matters. Mr. Cook earned his J.D. from Harvard Law School in 1992, a Master of Science in Industrial Relations and Personnel Management from the London School of Economics in 1989, and an A.B. in Social Studies from Harvard College in 1988.

Speakers:

Roel C. Campos is senior counsel in the firm's Washington, DC, office. Mr. Campos' practice consists of advising senior management and boards in their most sensitive and complex issues. His practice often involves conducting internal investigations and defending matters involving financial regulators, such as the SEC, DOJ, CFTC, and FINRA. He also advises boards on items such as cybersecurity, governance, cryptocurrency and proposed rulemakings by financial regulators. Beginning in 2002, Mr. Campos was appointed twice by President George W. Bush and confirmed by the US Senate as a Commissioner of the SEC, serving until 2007. During his tenure, Mr. Campos presided over hundreds of complex enforcement cases and rulemakings, involving the full range of federal securities laws. Prior to being appointed to the SEC, Mr. Campos raised venture capital with partners, was a senior executive and operated a radio broadcasting company. He began his career after graduating from the US Air Force Academy and served as an officer for five years. After attending Harvard Law School, he worked in Los Angeles for major law firms as a corporate transactions/securities lawyer and litigator. Mr. Campos served in the US Attorney's Office in Los Angeles. He prosecuted major narcotics cartels and, in a celebrated trial, convicted several kingpin cartel members for the kidnapping and murder of a DEA.

Audria Pendergrass Lee is FINRA's Vice President of Talent Acquisition and Chief Diversity Officer. In this role, she leads FINRA's strategic diversity, equity and inclusion, and talent acquisition efforts. Since joining FINRA in 2009, Ms. Lee has spearheaded the strategic deployment of resources that support FINRA's goal of fostering an attractive and inclusive workplace. Before assuming her current role, she served in various positions, where she helped to facilitate the creation of an award-winning diversity leadership council and employee resource group program; launched formal mentoring programs; oversaw the implementation of organization-wide diversity education; and made significant enhancements to flexible work arrangements, gender- and LGBTQ-inclusive policies and other diversity programming efforts. In 2019, Ms. Lee was recognized by *The Network Journal* as an Influential Black Woman in Business. She also serves on the board of the Center for Workforce Compliance and as a member of the Tanenbaum Workplace Advisory Council. Prior to joining FINRA, Ms. Lee worked as a diversity program manager, new service development director and paralegal in a variety of industries, including the military, financial services, distribution and educational services. Ms. Lee, a Life Member of Alpha Kappa Alpha Sorority, Inc., earned

her Bachelor of Arts in Political Science from the University of South Carolina, and her master's degree in Organizational Management from the University of Phoenix. She has continued her studies at the University of Maryland University College and Aresty Institute of Executive Education at The Wharton School, University of Pennsylvania.

Diversity and Inclusion

Speakers

- **Introduction**
  - Robert Cook, President and Chief Executive Officer, FINRA
- **Speakers**
  - Roel C. Campos, Senior Counsel, Hughes Hubbard & Reed LLP
  - Audria Pendergrass Lee, Vice President, Talent Acquisition and Chief Diversity Officer, FINRA Human Resources

Market Structure: What Factors Are Driving Changes

Tuesday, May 17, 2022
4:15 p.m. – 5:15 p.m.

During this session, FINRA staff and industry practitioners discuss current developments and future trends in the industry, including best execution guidance and payment for order flow issues.

Moderator:

Patrick Geraghty
Vice President, Fixed Income, Offerings, & Customer Issues (FIOCI)
FINRA Market Regulation

Panelists:

Scott Kloin
Managing Director, Chief Compliance Officer & Senior Deputy General Counsel
Citadel Securities

Racquel Russell
Senior Vice President and Director Capital Markets
FINRA Office of General Counsel

Richard Wallace
Senior Vice President and Associate General Counsel
LPL Financial

Market Structure: What Factors Are Driving Changes Panelists Bios:

Moderator:

Patrick Geraghty is Vice President of the Fixed Income, Offerings and Customer Issues Group (FIOCI), providing operational management of the fixed income surveillance program and certain customer protection surveillance patterns for equities. The position oversees the fixed income teams, which conduct customer protection, market manipulation, and data-integrity surveillance patterns for TRACE-eligible and municipal securities. The position is also responsible for best execution, trading ahead surveillance patterns for equities. Mr. Geraghty works with internal and external groups including the SEC, the MSRB, the Federal Reserve Bank of NY, and the Treasury Department. Mr. Geraghty started with NASD in 1995 working in the real-time surveillance area, handling backing away complaints, trade reporting questions and locked crossed market issues. Mr. Geraghty then managed the Trading Practices and Customer Issues sections, which conducted surveillance for best execution, limit order protection and ITS/CAES trade-throughs, along with providing secondary offering surveillance under Regulation M. Mr. Geraghty also served as an advisor to the NASD Series 55 Committee during the development of the question bank for the exam. He took over the fixed income surveillance program in 2005 and has led the area through multiple expansions of TRACE to include agency debentures, asset-backed securities, mortgage-backed securities, and U.S. Treasury securities. Mr. Geraghty has a bachelor's degree in economics from Duke University.

Panelists:

Scott Kloin is Managing Director, Chief Compliance Officer & Senior Deputy General Counsel for Citadel Securities, a market maker in a broad array of equities and fixed income products. In this role, Mr. Kloin is responsible for leading the firm's compliance program and for promoting a culture of compliance and high integrity throughout the firm. Mr. Kloin and his team advise on all aspects of the laws, rules, regulations and best practices pertaining to sales, trading, quantitative research, technology, controls, and operations involving equities, listed options, futures, FX, US Treasuries, swaps. Prior to joining Citadel Securities in 2012, Mr. Kloin was Executive Director, Head of U.S. Equities Compliance of UBS Investment Bank, a full-service institutional equities broker-dealer and retail market maker. Prior to joining UBS, he was Vice President & Assistant General Counsel of JPMorgan Securities and an Associate in the financial services practice group of the law firm of Kelley Drye & Warren LLP. He earned a B.S. in Finance from the University of Maryland—College Park and a J.D. from the University of Miami and is a member of the New York and Connecticut Bars. He formerly chaired FINRA's Market Regulation Committee.

Racquel Russell is Senior Vice President and Director of Capital Markets in FINRA's Office of General Counsel (OGC). In this role, Ms. Russell oversees the Capital Markets Office as it develops new policy initiatives, provides counsel to the Department of Market Regulation and Transparency Services, and supports the fixed income examinations of the Member Supervision Department. She also provides expert guidance to the FINRA Board of Governors and senior management. Ms. Russell joined OGC in 2008 and previously served as an Associate General CounsFel and an Assistant General Counsel. Prior to joining FINRA, Ms. Russell was a Vice President in the Legal and Compliance Department at J.P. Morgan, London, UK. She also worked in a variety of legal roles at the U.S. Securities and Exchange Commission, including as a Branch Chief for Trading Practices in the Division of Trading and Markets. Ms. Russell earned a B.A. in Psychology from Canisius College and J.D. and M.B.A. degrees from the State University of New York at Buffalo, School of Law and School of Management.

Richard G. Wallace is Senior Vice President and Assistant General Counsel at LPL Financial LLC, a registered broker-dealer and investment advisor. He provides legal advice on trading and operational issues. Previously Mr. Wallace was a Vice President at FINRA where he oversaw the department's legal group, handling enforcement and policy issues. He also worked in the Enforcement Division of the U.S. Securities and Exchange Commission in Washington, D.C. As a partner at Foley & Lardner LLC, Mr. Wallace represented brokerage firms on market structure issues.

Market Structure: What Factors Are Driving Changes

Panelists

- **Moderator**
  - Patrick Geraghty, Vice President, Fixed Income, Offerings, & Customer Issues (FIOCI), FINRA Market Regulation
- **Panelists**
  - Scott Kloin, Managing Director, Chief Compliance Officer & Senior Deputy General Counsel, Citadel Securities
  - Racquel Russell, Senior Vice President and Director Capital Markets, FINRA Office of General Counsel
  - Richard Wallace, Senior Vice President and Associate General Counsel, LPL Financial

Market Structure: What Factors Are Driving Changes
Tuesday, May 17, 2022
4:15 p.m. – 5:15 p.m.

Resources:

FINRA Resources:

- FINRA *Regulatory Notice 22-04, FINRA Reminds Member Firms of Obligation to Execute Marketable Customer Orders Fully and Promptly* (January 2022)

  www.finra.org/rules-guidance/notices/22-04

- FINRA *Regulatory Notice 21-35, FINRA Requests Comment on Proposed Order Routing Disclosure Requirements for OTC Equity Securities and Potential Steps to Facilitate Investor Access to Current Order Routing Disclosures for NMS Securities* (October 2021)

  www.finra.org/rules-guidance/notices/21-35

- FINRA *Regulatory Notice 21-23, FINRA Reminds Member Firms of Requirements Concerning Best Execution and Payment for Order Flow* (June 2021)

  www.finra.org/rules-guidance/notices/21-23

- FINRA *Regulatory Notice 15-46, Guidance on Best Execution Obligations in Equity, Options and Fixed Income Markets* (November 2015)

  www.finra.org/rules-guidance/notices/15-46

- FINRA *Regulatory Notice 14-54, FINRA Reminds Firms of Extended Hours Trading Disclosures* (December 2014)

  www.finra.org/rules-guidance/notices/14-54

SEC Resources:

- Securities and Exchange Commission Rule, *Market Data Infrastructure Rule* (Effective date: June 2021)

  www.sec.gov/rules/final/2020/34-90610.pdf

- Securities and Exchange Commission *Proposal, Further Definition of "As a Part of a Regular Business" in the Definition of Dealer and Government Securities Dealer* (March 2022)

  www.sec.gov/rules/proposed/2022/34-94524.pdf

- Securities and Exchange Commission *Proposal, Shortening the Securities Transaction Settlement Cycle* (February 2022)

  www.sec.gov/rules/proposed/2022/34-94196.pdf

- Securities and Exchange Commission *Proposal, Amendments Regarding the Definition of "Exchange" and Alternative Trading Systems (ATSs) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities* (January 2022)

  www.sec.gov/rules/proposed/2022/34-94062.pdf

- Securities and Exchange Commission Speech, *"The Names Bond": Remarks at City Week by Chair Gary Gensler* (April 26, 2022)

  www.sec.gov/news/speech/gensler-names-bond-042622

FINRA's Membership Application Program (MAP)
Tuesday, May 17, 2022
4:15 p.m. – 5:15 p.m.

Attend this session to hear about FINRA's Membership Application Program (MAP). Learn how FINRA evaluates proposed business activities of potential and existing member firms, including the applicant's financial, operational, supervisory and compliance systems. This session provides an overview of the application process.

Moderator:
Cindy Foster
Vice President, Membership Application Program & Statutory Disqualification
FINRA Member Supervision

Panelists:
Leyna Goro
Senior Director, Retail Membership Application Program
FINRA Member Supervision

Eda Henries
Founder and Principal
Henries & Co.

John Sakhleh
Partner, Securities Enforcement and Regulatory Group
Sidley Austin, LLP

FINRA's Membership Application Program (MAP) Panelists Bios:

Moderator:

Cindy Foster is Vice President of the FINRA Membership Application Program and Statutory Disqualification. Ms. Foster provides strategic leadership to the group responsible for assessing the proposed business activities of potential and current member firms and evaluating applicants' financial, operational, supervisory, and compliance systems. Ms. Foster also oversees the assessment of applications for firms and individuals who are subject to statutory disqualification and making recommendations to approve or deny the applications to the National Adjudicatory Council. Prior to joining MAP, Ms. Foster had been FINRA's Ombudsman since 2009. In that role, Ms. Foster worked with a cross-section of securities industry to review and resolve concerns and complaints arising from examinations, investigations, arbitrations, and FINRA's disciplinary process. Prior to that role, Ms. Foster served in various capacities at FINRA, including as a Market Regulation senior analyst responsible for investigating manipulation and fraud in the over-the-counter securities markets, as Associate Director and Lead for the Order Audit Trail System (OATS) Member Firm Coordination Project, and as a Senior Director in Member Relations. In 2000, Ms. Foster joined a financial services software company, SunGard Trading Systems/BRASS (STS), where she served in senior capacities, including Chief Compliance Officer and Executive Vice President, before rejoining FINRA in 2006. At STS she advised executive management on the impact of securities industry rules and regulations on the company's order management and trade execution systems and interfaced with the firm's clients across a range of issues. Her role at STS grew over time to include responsibility for Product Management, Technology, and Client Services. Ms. Foster has Master of Business Administration and Master of Science degrees from the University of Maryland University College. She previously served on FINRA's Pension/401(k) Committee and is an inaugural member and former Chair of FINRA's Diversity Leadership Council. She also served as Executive Sponsor for FINRA's Latino Employee Relationship Group and as a member of FINRA's Racial Justice Task Force.

Panelists:

Leyna Goro is Senior Director in the FINRA Membership Application Program (MAP) group. Ms. Goro oversees the team responsible for analyzing membership filings from current and proposed FINRA firms in the Retail firm group. She plays a key strategic role in the oversight of firm business activities in this area, including complex and novel matters. Ms. Goro also provides insight to FINRA constituents on the membership process, in areas such as compliance, securities products, Anti-Money Laundering, risk assessments, and structural changes. Ms. Goro has served as an expert speaker on industry panels, and frequently interfaces with regulatory agencies on topics impacting the FINRA membership space. Ms. Goro was previously an Associate Director in MAP, and before that, held various positions at FINRA, including MAP supervisor, as well as examiner in the cycle and application review programs. Ms. Goro has played a significant role in several high-profile initiatives, including process innovation and technology elements of MAP's recent transition to a new organizational structure, the implementation and rollout of FINRA Rule 1017(a)(7), and FINRA's retrospective review of the MAP rules. She has served as a FINRA National Regulatory Expert, completed the FINRA Excellence in Management Program at Wharton, and currently serves as a Co-Chair on FINRA Women's Network Career Development Subcommittee.

Eda Henries, Founder and Principal, leads Henries & Co., a boutique firm that provides investment banking and strategic advisory services to small and emerging privately held companies. Ms. Henries has 15+ years of entrepreneurial, advisory and investment experience in the U.S. and Africa. Her past roles include Principal at an early-stage investment firm, Vice President in Citigroup's Investment Banking division and co-founder and operator of food service and agribusiness ventures in West Africa. She is a Georgetown and Columbia Business School alumna and a board member of the Brooklyn Kindergarten Society.

John Sakhleh is a partner in the Securities Enforcement and Regulatory group, which received the 2019 *Chambers USA* Award for Financial Services Regulation Firm of the Year and was named the Law Firm of the Year for Securities Regulation in 2020 and 2017 by *U.S. News – Best Lawyers*. Mr. Sakhleh advises a wide array of financial services firms including investment and commercial banks, broker-dealers, investment advisers and private/hedge funds — on a broad variety of regulatory, enforcement, compliance and transactional matters. Mr. Sakhleh regularly advises on transactions involving U.S. and non-U.S. financial services and FinTech companies. His experience includes advising on transactional and regulatory matters in connection with merger and acquisitions of broker-dealers, investment advisers and other FinTech companies. These complex projects include advising on compliance-related integration issues, technology conversions of systems, migration of customer accounts and trading platforms, restructuring of major business units and obtaining the necessary regulatory approvals in strategic transactions. Mr. Sakhleh also advises numerous financial institutions on trading and technology platforms in connection with (i) evaluating the broker-dealer and investment adviser registration requirements, and (ii) advising on the formation and regulatory approval process for newly formed broker-dealers and investment advisers with the SEC, FINRA, other self-regulatory organizations and clearing agencies. Mr. Sakhleh's regulatory and compliance-related practice includes advising clients on general broker-dealer registration and SRO membership, dealer/trader/finder issues, FinTech/trading platforms, clearing firms and related financial responsibility requirements, FINRA advertising rules, Regulation BI, outsourcing arrangements and non U.S. broker-dealer/cross-border registration requirements (Rule 15a-6 and related no-action letters), books and records/electronic recordkeeping issues, Regulation ATS and supervisory liability for CCOs and senior officers. Mr. Sakhleh's practice also includes a concentration on enforcement defense and regulatory counseling matters, in which he brings to bear his extensive knowledge of the regulatory schemes governing securities market and regulatory issues for broker-dealers, investment advisers, investment funds and FinTech trading platforms. His securities enforcement practice has covered a broad range of enforcement matters, including investigations of securities fraud, investment adviser misconduct, broker-dealer matters, municipal bond-related trading, capital deficiencies, conversion/integration issues and trading-related investigations, including spoofing. Mr. Sakhleh has defended a wide variety of clients in investigations before the U.S. Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), the Commodity Futures Trading Commission (CFTC) and the National Futures Association (NFA). Prior to joining the firm, Mr. Sakhleh worked for the SEC's Office of Compliance Inspections and Examinations. During his time with the SEC, Mr. Sakhleh was involved with, among other things, the SEC's market-timing and late trading, proprietary trading and best execution investigations and examinations. Prior to joining the SEC, Mr. Sakhleh worked for a national law firm where he focused on investment company, investment adviser and hedge fund-related issues. Mr. Sakhleh also worked at a large national accounting firm as a Certified Public Accountant (inactive).

FINRA's Membership Application Program (MAP)

Panelists

- **Moderator**
  - Cindy Foster, Vice President, Membership Application Program & Statutory Disqualification, FINRA Member Supervision
- **Panelists**
  - Leyna Goro, Senior Director, Retail Membership Application Program, FINRA Member Supervision
  - Eda Henries, Founder and Principal, Henries & Co.
  - John Sakhleh, Partner, Securities Enforcement and Regulatory Group, Sidley Austin, LLP

FINRA's Membership Application Program (MAP)
Tuesday, May 17, 2022
4:15 p.m. – 5:15 p.m.

Resources:

- FINRA *Information Notice, FINRA Membership Application Program Transformation* (April 2022)

  www.finra.org/sites/default/files/2022-04/Information-Notice-041922.pdf

- FINRA Unscripted: MAP Transformation: Streamlining FINRA's Gatekeeper Function (April 2022)

  www.finra.org/media-center/finra-unscripted/membership-application-program-transformation

- MAP Intake Contact Info: As part of MAP's ongoing transformation, the group has implemented a new centralized MAP Intake function to provide enhanced support to applicants prior to filing. Please note the following new contacts for such calls, meetings and requests:
  - Dedicated telephone number: (212) 858-4000 (Option 5 – Membership Applications)
  - Email address *MAPIntake@finra.org*

Cybersecurity: Emerging Industry Priorities and Threats
Tuesday, May 17, 2022
4:15 p.m. – 5:15 p.m.

Cyber threats are no longer a question of if, but when, a breach will occur. It is important to have a cybersecurity plan in place, so you are ready to act if your organization experiences a data breach. Join panelists as they share areas of focus for the year ahead.

Moderator:
Brita Bayatmakou
Senior Director, Cyber and Analytics Unit (CAU)
FINRA Member Supervision

Panelists:
Brian Carter
Vice President, Technology
Sigma Financial

David Kelley
Director, Cyber and Analytics Unit (CAU)
FINRA Member Supervision

Bryan Smith
Section Chief, Cyber Criminal Section
Federal Bureau of Investigation (FBI)

Cybersecurity: Emerging Industry Priorities and Threats Panelists Bios:

Moderator:

Brita Bayatmakou is Senior Director in FINRA's National Cause and Financial Crimes Detection Program where she leads the Cyber and Analytics Unit. Her team's mission is to assess and enhance member firms' cyber controls, support firm examination teams, and conduct complex investigations in the cybersecurity and cyber-enabled fraud disciplines, including crypto-related assets. Additionally, she leads the department's data analytics and technology strategy, which helps to proactively target top financial crime-related threats. Ms. Bayatmakou joined FINRA from Charles Schwab where she built out several functions within the Financial Crimes Risk Management organization including an intelligence team that analyzed and identified emerging and complex fraud, AML and sanctions evasion trends. She also led a team that focused on financial crime threat detection through the use of data science and advanced analytics. Reflecting her AML expertise, Ms. Bayatmakou served as the BSA/AML Officer of Schwab's Mutual Funds, ETFs, Worldwide Funds PLC and Charles Schwab Futures, Inc. Ms. Bayatmakou has authored/co-authored several publications related to financial crimes, cybersecurity, and AML topics. She holds two Masters Degrees, is a Certified Financial Crimes Specialist (CFCS), and Certified Anti-Money Laundering Specialist (CAMS). In addition to English, Ms. Bayatmakou speaks French, Farsi, and Arabic.

Panelists:

Brian Carter is Vice President of Technology for Sigma Financial Corporation and Parkland Securities, LLC. He joined the firm in early 2021 to lead the effort to modernize and transform their technology platform. Mr. Carter brings a passion for implementing technology that helps organizations and people be more effective. How can we create solutions that allow people to shift their time from doing lower-value work to higher-value work? In the Post-COVID World with people working remotely, how do we allow them to do their work effectively while mitigating the constant cybersecurity threats posed by bad actors? These are some of the questions Mr. Carter thinks the most about. He began his 20 plus years of experience in financial services technology as a programmer tasked with building a new commission processing system for National Planning Holdings, a broker dealer network formerly owned by Jackson National Life. From there he moved into various leadership roles, gaining experience in a wide range of technology disciplines. Mr. Carter earned an MBA from Vanderbilt University in 2014, which was a catalyst to transforming his outlook on technology to be more business focused.

Dave Kelley, Director, Member Supervision Specialist Programs, is based out of FINRA's Kansas City office. He has been with FINRA for more than 11 years and leads the specialist team dealing with cybersecurity and information technology controls. Prior to joining FINRA, he worked for more than 19 years at American Century Investments in various positions, including Chief Privacy Officer, Director of IT Audit, Director of Electronic Commerce Controls and AML Officer. He led the development of website controls, including customer application security, ethical hacking programs and application controls. Mr. Kelley is a CPA and Certified Internal Auditor, and previously held the Series 7 and 24 licenses.

Bryan Smith has been employed by the Federal Bureau of Investigation (FBI) as a Special Agent since 2002 and currently serves as the Section Chief for the FBI's Cyber Criminal Section where he is responsible for the FBI's investigations and operations against cybercriminal actors and threats. Prior to his current role, Mr. Smith served as the Assistant Special Agent in Charge over the Cleveland Field Office's Cyber/White Collar Branch, Unit Chief over the FBI's Money Laundering and Bank Fraud unit, and as the FBI's Detailee to the U.S. Securities and Exchange Commission (SEC) where he assisted both agencies in insider trading, market manipulation, and investment fraud matters. His experience crosses over financial crimes, cyber, and virtual currency and he has initiated a number of private sector outreach efforts to better

leverage the complementary knowledge of both. Prior to the FBI, Mr. Smith worked as a consultant for Accenture and Deloitte and Touche and is a graduate of Bradley University with a degree in accounting.

Cybersecurity: Emerging Industry Priorities and Threats

Panelists

- **Moderator**
  - Brita Bayatmakou, Senior Director, Cyber and Analytics Unit (CAU), FINRA Member Supervision
- **Panelists**
  - Brian Carter, Vice President, Technology, Sigma Financial
  - David Kelley, Director, Cyber and Analytics Unit (CAU), FINRA Member Supervision
  - Bryan Smith, Section Chief, Cyber Criminal Section, Federal Bureau of Investigation (FBI)

To Access Polling

- **Please get your devices out:**
  - Type the polling address, **https://finra.cnf.io/sessions/a6eh** into the browser or scan the QR code with your camera.

  - Select your polling answers.

Polling Question 1

1. **From a cyber threat perspective, which of the following most keeps you up at night?**
   a. An email phishing attack
   b. The possibility of a ransomware attack
   c. Unauthorized customer account access and theft
   d. A widespread cyber attack on critical infrastructure
   e. Other cyber issue

Polling address: **https://finra.cnf.io/sessions/a6eh**

Polling Question 2

2. **Do you have an established contact within the law enforcement community who you would call if/when a cyber event occurs?**
   a. Yes, the FBI
   b. Yes, the local police
   c. No
   d. I would have to go dig up a business card in the bottom of my desk drawer

Polling address: **https://finra.cnf.io/sessions/a6eh**

Polling Question 3

3. **Have you already implemented some form of multi-factor authentication (MFA)?**
   a. Yes, our firm uses MFA to verify customers when they access accounts online.
   b. Yes, our firm requires employees and reps to use MFA (e.g., for external access to email systems or to access systems that may contain confidential information).
   c. Yes, our firm uses MFA for employees, reps and customers.
   d. No, we don't use MFA today.

Polling address: **https://finra.cnf.io/sessions/a6eh**

Cybersecurity: Emerging Industry Priorities and Threats
Tuesday, May 17, 2022
4:15 p.m. – 5:15 p.m.

Resources:

- FINRA *Regulatory Notice 21-18, FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts* (May 2021)

  www.finra.org/rules-guidance/notices/21-18

- FINRA *Information Notice – 4/29/19, Imposter Websites Impacting Member Firms* (April 2019)

  www.finra.org/rules-guidance/notices/information-notice-042919

Alert (AA22-110A)

More Alerts

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

Original release date: April 20, 2022

Summary

The cybersecurity authorities of the United States[1][2][3], Australia[4], Canada[5(link is external)], New Zealand[6], and the United Kingdom[7][8] are releasing this joint Cybersecurity Advisory (CSA). The intent of this joint CSA is to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners.

Actions critical infrastructure organizations should implement to immediately protect against Russian state-sponsored and criminal cyber threats:
• Patch all systems. Prioritize patching known exploited vulnerabilities.
• Enforce multifactor authentication.
• Secure and monitor Remote Desktop Protocol and other risky services.
• Provide end-user awareness and training.

Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks (see the March 21, 2022, Statement by U.S. President Biden for more information). Recent Russian state-sponsored cyber operations have included distributed denial-of-service (DDoS) attacks, and older operations have included deployment of destructive malware against Ukrainian government and critical infrastructure organizations.

Additionally, some cybercrime groups have recently publicly pledged support for the Russian government. These Russian-aligned cybercrime groups have threatened to conduct cyber operations

in retaliation for perceived cyber offensives against the Russian government or the Russian people. Some groups have also threatened to conduct cyber operations against countries and organizations providing materiel support to Ukraine. Other cybercrime groups have recently conducted disruptive attacks against Ukrainian websites, likely in support of the Russian military offensive.

This advisory updates joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure, which provides an overview of Russian state-sponsored cyber operations and commonly observed tactics, techniques, and procedures (TTPs). This CSA—coauthored by U.S., Australian, Canadian, New Zealand, and UK cyber authorities with contributions from industry members of the Joint Cyber Defense Collaborative (JCDC)—provides an overview of Russian state-sponsored advanced persistent threat (APT) groups, Russian-aligned cyber threat groups, and Russian-aligned cybercrime groups to help the cybersecurity community protect against possible cyber threats.

U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities urge critical infrastructure network defenders to prepare for and mitigate potential cyber threats—including destructive malware, ransomware, DDoS attacks, and cyber espionage—by hardening their cyber defenses and performing due diligence in identifying indicators of malicious activity. Refer to the Mitigations section of this advisory for recommended hardening actions.

For more information on Russian state-sponsored cyber activity, see CISA's Russia Cyber Threat Overview and Advisories webpage. For more information on the heightened cyber threat to critical infrastructure organizations, see the following resources:

- Cybersecurity and Infrastructure Security Agency (CISA) Shields Up and Shields Up Technical Guidance webpages
- Australian Cyber Security Centre's (ACSC) Advisory Australian Organisations Should Urgently Adopt an Enhanced Cyber Security Posture.
- Canadian Centre for Cyber Security (CCCS) Cyber Threat Bulletin Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity(link is external)
- National Cyber Security Centre New Zealand (NZ NCSC) General Security Advisory Understanding and preparing for cyber threats relating to tensions between Russia and Ukraine
- United Kingdom's National Cyber Security Centre (NCSC-UK) guidance on how to bolster cyber defences in light of the Russian cyber threat

Click here for a PDF version of this report.

Technical Details

Russian State-Sponsored Cyber Operations

Russian state-sponsored cyber actors have demonstrated capabilities to compromise IT networks; develop mechanisms to maintain long-term, persistent access to IT networks; exfiltrate sensitive data from IT and operational technology (OT) networks; and disrupt critical industrial control systems (ICS)/OT functions by deploying destructive malware.
Historical operations have included deployment of destructive malware—including BlackEnergy and NotPetya—against Ukrainian government and critical infrastructure organizations. Recent Russian

state-sponsored cyber operations have included DDoS attacks against Ukrainian organizations. **Note:** for more information on Russian state-sponsored cyber activity, including known TTPs, see joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure.

Cyber threat actors from the following Russian government and military organizations have conducted malicious cyber operations against IT and/or OT networks:

- **The Russian Federal Security Service (FSB), including FSB's Center 16 and Center 18**
- **Russian Foreign Intelligence Service (SVR)**
- **Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS)**
- **GRU's Main Center for Special Technologies (GTsST)**
- **Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)**

The Russian Federal Security Service

Overview: FSB, the KGB's successor agency, has conducted malicious cyber operations targeting the Energy Sector, including UK and U.S. energy companies, U.S. aviation organizations, U.S. government and military personnel, private organizations, cybersecurity companies, and journalists. FSB has been known to task criminal hackers for espionage-focused cyber activity; these same hackers have separately been responsible for disruptive ransomware and phishing campaigns.

Industry reporting identifies three intrusion sets associated with the FSB, but the U.S. and UK governments have only formally attributed one of these sets—known as BERSERK BEAR—to FSB.

- **BERSERK BEAR (also known as Crouching Yeti, Dragonfly, Energetic Bear, and Temp.Isotope)** has, according to industry reporting, historically targeted entities in Western Europe and North America including state, local, tribal, and territorial (SLTT) organizations, as well as Energy, Transportation Systems, and Defense Industrial Base (DIB) Sector organizations. This group has also targeted the Water and Wastewater Systems Sector and other critical infrastructure facilities. Common TTPs include scanning to exploit internet-facing infrastructure and network appliances, conducting brute force attacks against public-facing web applications, and leveraging compromised infrastructure—often websites frequented or owned by their target—for Windows New Technology Local Area Network Manager (NTLM) credential theft. Industry reporting assesses that this actor has a destructive mandate.

The U.S. and UK governments assess that this APT group is almost certainly FSB's Center 16, or Military Unit 71330, and that FSB's Center 16 has conducted cyber operations against critical IT systems and infrastructure in Europe, the Americas, and Asia.

Resources: for more information on BERSERK BEAR, see the MITRE ATT&CK® webpage on Dragonfly.

High-Profile Activity: in 2017, FSB employees, including one employee in the FSB Center for Information Security (also known as Unit 64829 and Center 18), were indicted by the U.S. Department of Justice (DOJ) for accessing email accounts of U.S. government and military personnel, private organizations, and cybersecurity companies, as well as email accounts of

journalists critical of the Russian government.[9] More recently, in 2021, FSB Center 16 officers were indicted by the U.S. DOJ for their involvement in a multi-stage campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data. One of the victims was a U.S. nuclear power plant.[10]

Resources: for more information on FSB, see:

- U.S. DOJ Press Release Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide
- Joint CSA Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector
- UK Press Release UK Exposes Russian Spy Agency Behind Cyber Incidents

Russian Foreign Intelligence Service

Overview: SVR has operated an APT group since at least 2008 that has targeted multiple critical infrastructure organizations. SVR cyber threat actors have used a range of initial exploitation techniques that vary in sophistication coupled with stealthy intrusion tradecraft within compromised networks. SVR cyber actors' novel tooling and techniques include:

- Custom, sophisticated multi-platform malware targeting Windows and Linux systems (e.g., GoldMax and TrailBlazer); and
- Lateral movement via the "credential hopping" technique, which includes browser cookie theft to bypass multifactor authentication (MFA) on privileged cloud accounts.[11(link is external)]

High-Profile Activity: the U.S. Government, the Government of Canada, and the UK Government assess that SVR cyber threat actors were responsible for the SolarWinds Orion supply chain compromise and the associated campaign that affected U.S. government agencies, critical infrastructure entities, and private sector organizations.[12][13(link is external)][14]

Also known as: APT29, COZY BEAR, CozyDuke, Dark Halo, The Dukes, NOBELIUM, and NobleBaron, StellarParticle, UNC2452, YTTRIUM [15]

Resources: for more information on SVR, see:

- Joint CSA Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders
- Joint Advisory Further TTPs associated with SVR cyber actors
- The MITRE ATT&CK webpage on APT29

For more information on the SolarWinds Orion supply chain compromise, see:

- CISA's Supply Chain Compromise webpage
- CISA's webpage on Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise
- NCSC-UK Guidance Dealing with the SolarWinds Orion compromise

GRU, 85th Main Special Service Center

Overview: GTsSS, or Unit 26165, is an APT group that has operated since at least 2004 and

primarily targets government organizations, travel and hospitality entities, research institutions, and non-governmental organizations, in addition to other critical infrastructure organizations.

According to industry reporting, GTsSS cyber actors frequently collect credentials to gain initial access to target organizations. GTsSS actors have collected victim credentials by sending spearphishing emails that appear to be legitimate security alerts from the victim's email provider and include hyperlinks leading to spoofed popular webmail services' logon pages. GTsSS actors have also registered domains to conduct credential harvesting operations. These domains mimic popular international social media platforms and masquerade as tourism- and sports-related entities and music and video streaming services.

High-Profile Activity: the U.S. Government assesses that GTsSS cyber actors have deployed Drovorub malware against victim devices as part of their cyber espionage operations.[16] The U.S. Government and UK Government assess that GTsSS actors used a Kubernetes® cluster to conduct widespread, distributed, and anonymized brute force access attempts against hundreds of government and private sector targets worldwide.[17]

Also known as: APT28, FANCY BEAR, Group 74, IRON TWILIGHT, PawnStorm, Sednit, SNAKEMACKEREL, Sofacy, STRONTIUM, Swallowtail, TG-4127, Threat Group-4127, and Tsar Team [18]

Resources: for more information on GTsSS, see the MITRE ATT&CK webpage on APT28.

GRU's Main Center of Special Technologies

Overview: GTsST, or Unit 74455, is an APT group that has operated since at least 2009 and has targeted a variety of critical infrastructure organizations, including those in the Energy, Transportation Systems, and Financial Services Sectors. According to industry reporting, GTsST also has an extensive history of conducting cyber espionage as well as destructive and disruptive operations against NATO member states, Western government and military organizations, and critical infrastructure-related organizations, including in the Energy Sector.

The primary distinguishing characteristic of the group is its operations use techniques aimed at causing disruptive or destructive effects at targeted organizations using DDoS attacks or wiper malware. The group's destructive operations have also leveraged wiper malware that mimics ransomware or hacktivism and can result in collateral effects to organizations beyond the primary intended targets. Some of their disruptive operations have shown disregard or ignorance of potential secondary or tertiary effects.

High-Profile Activity: the malicious activity below has been previously attributed to GTsST by the U.S. Government and the UK Government.[19][20]

- GTsST actors conducted a cyberattack against Ukrainian energy distribution companies in December 2015, leading to disruption of multiple companies' operations and widespread temporary outages. The actors deployed BlackEnergy malware to steal user credentials and used BlackEnergy's destructive component, KillDisk, to make infected computers inoperable.
- In 2016, GTsST actors conducted a cyber-intrusion campaign against a Ukrainian electrical transmission company and deployed CrashOverride malware (also known as Industroyer) specifically designed to attack power grids.

- In June 2017, GTsST actors deployed NotPetya disruptive malware against Ukrainian financial, energy, and government organizations. NotPetya masqueraded as ransomware, had a large collateral impact, and caused damage to millions of devices globally.
- In 2018, GTsST actors deployed data-deletion malware against the Winter Olympics and Paralympics using VPNFilter.

The U.S. Government, the Government of Canada, and UK Government have also attributed the October 2019 large-scale, disruptive cyber operations against a range of Georgian web hosting providers to GTsST. This activity resulted in websites—including sites belonging to the Georgian government, courts, non-government organizations (NGOs), media, and businesses—being defaced and interrupted the service of several national broadcasters.[21]22(link is external)][23]

Also known as: ELECTRUM, IRON VIKING, Quedagh, the Sandworm Team, Telebots, VOODOO BEAR [24]

Resources: for more information on GTsST, see the MITRE ATT&CK webpage on Sandworm Team.

Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics

Overview: TsNIIKhM, as described on their webpage, is a research organization under Russia's Ministry of Defense (MOD). Actors associated with TsNIIKhM have developed destructive ICS malware.

High-Profile Activity: TsNIIKhM has been sanctioned by the U.S. Department of the Treasury for connections to the destructive Triton malware (also called HatMan and TRISIS); TsNIIKhM has been sanctioned by the UK Foreign, Commonwealth, and Development Office (FCDO) for a 2017 incident that involved safety override controls (with Triton malware) in a foreign oil refinery.[25][26] In 2021, the U.S. DOJ indicted a TsNIIKhM Applied Development Center (ADC) employee for conducting computer intrusions against U.S. Energy Sector organizations. The indicted employee also accessed the systems of a foreign oil refinery and deployed Triton malware.[27] Triton is a custom-built malware designed to manipulate safety instrumented systems within ICS controllers, disabling the safety alarms that prevent dangerous conditions.

Also known as: Temp.Veles, XENOTIME [28]

Resources: for more information on TsNIIKhM, see the MITRE ATT&CK webpage on TEMP.Veles. For more information on Triton, see:

- CISA Malware Analysis Report (MAR) Hatman – Safety System Targeted Malware (update B)
- CISA ICS Advisory: Schneider Electric Triconex Tricon (Update B)
- Joint CSA Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector
- NCSC-UK Advisory TRITON Malware Targeting Safety Controllers

Russian-Aligned Cyber Threat Groups

In addition to the APT groups identified in the Russian State-Sponsored Cyber Operations section, industry reporting identifies two intrusion sets—PRIMITIVE BEAR and VENOMOUS BEAR—as state-sponsored APT groups, but U.S., Australian, Canadian, New Zealand, and UK cyber authorities have

not attributed these groups to the Russian government.

- **PRIMITIVE BEAR** has, according to industry reporting, targeted Ukrainian organizations since at least 2013. This activity includes targeting Ukrainian government, military, and law enforcement entities using high-volume spearphishing campaigns to deliver its custom malware. According to industry reporting, PRIMITIVE BEAR conducted multiple cyber operations targeting Ukrainian organizations in the lead up to Russia's invasion.

Resources: for more information on PRIMITIVE BEAR, see the MITRE ATT&CK webpage on the Gamaredon Group.

- **VENOMOUS BEAR** has, according to industry reporting, historically targeted governments aligned with the North Atlantic Treaty Organization (NATO), defense contractors, and other organizations of intelligence value. Venomous Bear is known for its unique use of hijacked satellite internet connections for command and control (C2). It is also known for the hijacking of other non-Russian state-sponsored APT actor infrastructure.[29] VENOMOUS BEAR has also historically leveraged compromised infrastructure and maintained an arsenal of custom-developed sophisticated malware families, which is extremely complex and interoperable with variants developed over time. VENOMOUS BEAR has developed tools for multiple platforms, including Windows, Mac, and Linux.[30(link is external)]

Resources: for more information on VENOMOUS BEAR, see the MITRE ATT&CK webpage on Turla.

Russian-Aligned Cybercrime Groups

Cybercrime groups are typically financially motivated cyber actors that seek to exploit human or security vulnerabilities to enable direct theft of money (e.g., by obtaining bank login information) or by extorting money from victims. These groups pose consistent threats to critical infrastructure organizations globally.

Since Russia's invasion of Ukraine in February 2022, some cybercrime groups have independently publicly pledged support for the Russian government or the Russian people and/or threatened to conduct cyber operations to retaliate against perceived attacks against Russia or materiel support for Ukraine. These Russian-aligned cybercrime groups likely pose a threat to critical infrastructure organizations primarily through:

- Deploying ransomware through which cyber actors remove victim access to data (usually via encryption), potentially causing significant disruption to operations.
- Conducting DDoS attacks against websites.
  - In a DDoS attack, the cyber actor generates enough requests to flood and overload the target page and stop it from responding.
  - DDoS attacks are often accompanied by extortion.
  - According to industry reporting, some cybercrime groups have recently carried out DDoS attacks against Ukrainian defense organizations, and one group claimed credit for DDoS attack against a U.S. airport the actors perceived as supporting Ukraine (see the Killnet section).

Based on industry and open-source reporting, U.S., Australian, Canadian, New Zealand, and UK

cyber authorities assess multiple Russian-aligned cybercrime groups pose a threat to critical infrastructure organizations. These groups include:

- **The CoomingProject**
- **Killnet**
- **MUMMY SPIDER**
- **SALTY SPIDER**
- **SCULLY SPIDER**
- **SMOKEY SPIDER**
- **WIZARD SPIDER**
- **The Xaknet Team**

Note: although some cybercrime groups may conduct cyber operations in support of the Russian government, U.S., Australian, Canadian, New Zealand, and UK cyber authorities assess that cyber criminals will most likely continue to operate primarily based on financial motivations, which may include targeting government and critical infrastructure organizations.

The CoomingProject

Overview: the CoomingProject is a criminal group that extorts money from victims by exposing or threatening to expose leaked data. Their data leak site was launched in August 2021.[31(link is external)] The CoomingProject stated they would support the Russian Government in response to perceived cyberattacks against Russia.[32(link is external)]

Killnet

Overview: according to open-source reporting, Killnet released a video pledging support to Russia.[33(link is external)]
Victims: Killnet claimed credit for carrying out a DDoS attack against a U.S. airport(link is external) in March 2022 in response to U.S. materiel support for Ukraine.[34(link is external)]

MUMMY SPIDER

Overview: MUMMY SPIDER is a cybercrime group that creates, distributes, and operates the Emotet botnet. Emotet is advanced, modular malware that originated as a banking trojan (malware designed to steal information from banking systems but that may also be used to drop additional malware and ransomware). Today Emotet primarily functions as a downloader and distribution service for other cybercrime groups. Emotet has been used to deploy WIZARD SPIDER's TrickBot, which is often a precursor to ransomware delivery. Emotet has worm-like features that enable rapid spreading in an infected network.

Victims: according to open sources, Emotet has been used to target industries worldwide, including financial, e-commerce, healthcare, academia, government, and technology organizations' networks.

Also known as: Gold Crestwood, TA542, TEMP.Mixmaster, UNC3443

Resources: for more information on Emotet, see joint Alert Emotet Malware. For more information on TrickBot, see joint CSA TrickBot Malware.

SALTY SPIDER

Overview: SALTY SPIDER is a cybercrime group that develops and operates the Sality botnet. Sality

is a polymorphic file infector that was discovered in 2003; since then, it has been replaced by more advanced peer-to-peer (P2P) malware loaders.[35(link is external)]

Victims: according to industry reporting, in February 2022, SALTY SPIDER conducted DDoS attacks against Ukrainian web forums used to discuss events relating to Russia's military offensive against the city of Kharkiv.

Also known as: Sality

SCULLY SPIDER

Overview: SCULLY SPIDER is a cybercrime group that operates using a malware-as-a-service model; SCULLY SPIDER maintains command and control infrastructure and sells access to their malware and infrastructure to affiliates, who distribute their own malware.[36(link is external)][37(link is external)] SCULLY SPIDER develops and operates the DanaBot botnet, which originated primarily as a banking Trojan but expanded beyond banking in 2021 and has since been used to facilitate access for other types of malware, including TrickBot, DoppelDridex, and Zloader. Like Emotet, Danabot effectively functions as an initial access vector for other malware, which can result in ransomware deployment.

According to industry reporting, recent DDoS activity by the DanaBot botnet suggests SCULLY SPIDER has operated in support of Russia's military offensive in Ukraine.

Victims: SCULLY SPIDER affiliates have primarily targeted organizations in the United States, Canada, Germany, United Kingdom, Australia, Italy, Poland, Mexico, and Ukraine.[38(link is external)] According to industry reporting, in March 2022, Danabot was used in DDoS attacks against multiple Ukrainian government organizations.

Also known as: Gold Opera

SMOKEY SPIDER

Overview: SMOKEY SPIDER is a cybercrime group that develops Smoke Loader (also known as Smoke Bot), a malicious bot that is used to upload other malware. Smoke Loader has been available since at least 2011, and operates as a malware distribution service for a number of different payloads, including—but not limited to—DanaBot, TrickBot, and Qakbot.

Victims: according to industry reporting, Smoke Loader was observed in March 2022 distributing DanaBot payloads that were subsequently used in DDoS attacks against Ukrainian targets.
Resources: for more information on Smoke Loader, see the MITRE ATT&CK webpage on Smoke Loader.

WIZARD SPIDER

Overview: WIZARD SPIDER is a cybercrime group that develops TrickBot malware and Conti ransomware. Historically, the group has paid a wage to the ransomware deployers (referred to as affiliates), some of whom may then receive a share of the proceeds from a successful ransomware attack. In addition to TrickBot, notable initial access and persistence vectors for affiliated actors include Emotet, Cobalt Strike, spearphishing, and stolen or weak Remote Desktop Protocol (RDP) credentials.

After obtaining access, WIZARD SPIDER affiliated actors have relied on various publicly available and otherwise legitimate tools to facilitate earlier stages of the attack lifecycle before deploying Conti ransomware.

WIZARD SPIDER pledged support to the Russian government and threatened critical infrastructure organizations of countries perceived to carry out cyberattacks or war against the Russian government.[39(link is external)] They later revised this pledge and threatened to retaliate against perceived attacks against the Russian people.[40(link is external)]

Victims: Conti victim organizations span across multiple industries, including construction and engineering, legal and professional services, manufacturing, and retail. In addition, WIZARD SPIDER affiliates have deployed Conti ransomware against U.S. healthcare and first responder networks.

Also known as: UNC2727, Gold Ulrick

Resources: for more information on Conti, see joint CSA Conti Ransomware. For more information on TrickBot, see joint CSA TrickBot Malware.

The XakNet Team

Overview: XakNet is a Russian-language cyber group that has been active as early as March 2022. According to open-source reporting, the XakNet Team threatened to target Ukrainian organizations in response to perceived DDoS or other attacks against Russia.[41(link is external)] According to reporting from industry, on March 31, 2022, XakNet released a statement stating they would work "exclusively for the good of [Russia]." According to industry reporting, the XakNet Team may be working with or associated with Killnet actors, who claimed credit for the DDoS attacks against a U.S. airport (see the Killnet section).

Victims: according to industry reporting, in late March 2022, the XakNet Team leaked email contents of a Ukrainian government official. The leak was accompanied by a political statement criticizing the Ukrainian government, suggesting the leak was politically motivated.

Mitigations

U.S., Australian, Canadian, New Zealand, and UK cyber authorities urge critical infrastructure organizations to prepare for and mitigate potential cyber threats by immediately (1) updating software, (2) enforcing MFA, (3) securing and monitoring RDP and other potentially risky services, and (4) providing end-user awareness and training.

- **Update software, including operating systems, applications, and firmware, on IT network assets.** Prioritize patching known exploited vulnerabilities and critical and high vulnerabilities that allow for remote code execution or denial-of-service on internet-facing equipment.
  - Consider using a centralized patch management system. For OT networks, use a risk-based assessment strategy to determine the OT network assets and zones that should participate in the patch management program.
  - Consider signing up for CISA's cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats. CISA's vulnerability scanning service evaluates external network presence by executing continuous scans of public, static IP addresses for accessible services and vulnerabilities.

- **Enforce MFA to the greatest extent possible and require accounts with password logins, including service accounts, to have strong passwords**. Do not allow passwords to be used across multiple accounts or stored on a system to which an adversary may have access. As Russian state-sponsored APT actors have demonstrated the ability to exploit default MFA protocols and known vulnerabilities, organizations should review configuration policies to protect against "fail open" and re-enrollment scenarios. For more information, see joint CSA Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability.
- **If you use RDP and/or other potentially risky services, secure and monitor them closely.** RDP exploitation is one of the top initial infection vectors for ransomware, and risky services, including RDP, can allow unauthorized access to your session using an on-path attacker.
  - Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a virtual private network (VPN) or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force attempts, log RDP login attempts, and disable unused remote access/RDP ports.
  - Ensure devices are properly configured and that security features are enabled. Disable ports and protocols that are not being used for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).
- **Provide end-user awareness and training** to help prevent successful targeted social engineering and spearphishing campaigns. Phishing is one of the top infection vectors for ransomware, and Russian state-sponsored APT actors have conducted successful spearphishing campaigns to gain credentials of target networks.
  - Ensure that employees are aware of potential cyber threats and delivery methods.
  - Ensure that employees are aware of what to do and whom to contact when they receive a suspected phishing email or suspect a cyber incident.

As part of a longer-term effort, **implement network segmentation to separate network segments based on role and functionality**. Network segmentation can help prevent the spread of ransomware and threat actor lateral movement by controlling traffic flows between—and access to—various subnetworks.

- Ensure OT assets are not externally accessible. Ensure strong identity and access management when OT assets needs to be externally accessible.
- Appropriately implement network segmentation between IT and OT networks. Network segmentation limits the ability of adversaries to pivot to the OT network even if the IT network is compromised. Define a demilitarized zone that eliminates unregulated communication between the IT and OT networks.
- Organize OT assets into logical zones by considering criticality, consequence, and operational necessity. Define acceptable communication conduits between the zones and deploy security controls to filter network traffic and monitor communications between zones. Prohibit ICS protocols from traversing the IT network.

To further prepare for and mitigate cyber threats from Russian state-sponsored or criminal actors, U.S., Australian, Canadian, New Zealand, and UK cyber authorities encourage critical infrastructure organizations to implement the recommendations listed below.

Preparing for Cyber Incidents

- Create, maintain, and exercise a cyber incident response and continuity of operations plan.
  - Ensure the cyber incident response plan contains ransomware- and DDoS-specific annexes. For information on preparing for DDoS attacks, see NCSC-UK guidance on preparing for denial-of-service attacks.
  - Keep hard copies of the incident response plan to ensure responders and network defenders can access the plan if the network has been shut down by ransomware, etc.
- Maintain offline (i.e., physically disconnected) backups of data. Backup procedures should be conducted on a frequent, regular basis (at a minimum every 90 days). Regularly test backup procedures and ensure that backups are isolated from network connections that could enable the spread of malware.
  - Ensure the backup keys are kept offline as well, to prevent them being encrypted in a ransomware incident.
- Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure with a particular focus on key data assets.
- Develop recovery documentation that includes configuration settings for common devices and critical equipment. Such documentation can enable more efficient recovery following an incident.
- Identify the attack surface by mapping and accounting all external-facing assets (applications, servers, IP addresses) that are vulnerable to DDoS attacks or other cyber operations.
- For OT assets/networks:
  - Identify a resilience plan that addresses how to operate if you lose access to—or control of—the IT and/or OT environment.
  - Identify OT and IT network interdependencies and develop workarounds or manual controls to ensure ICS networks can be isolated from IT networks if the connections create risk to the safe and reliable operation of OT processes. Regularly test contingency plans, such as manual controls, so that safety-critical functions can be maintained during a cyber incident. Ensure that the OT network can operate at necessary capacity even if the IT network is compromised.
  - Regularly test manual controls so that critical functions can be kept running if ICS or OT networks need to be taken offline.
  - Implement data backup procedures.
  - Develop recovery documents that include configuration settings for common devices and critical OT equipment.

Identity and Access Management

- Require accounts with password logins, including service accounts, to have strong passwords and do not allow passwords to be used across multiple accounts or stored on a system to which an adversary may have access. Consider using a password manager; see NCSC-UK's Password Manager Buyers Guide for guidance.
- Implement authentication timeout and lockout features to prevent repeated failed login attempts

and successful brute-force attempts.
- Create a deny list of known compromised credentials and prevent users from using known-compromised passwords.
- Secure credentials by restricting where accounts and credentials can be used and by using local device credential protection features. Russian state-sponsored APT actors have demonstrated their ability to maintain persistence using compromised credentials.
  - Use virtualizing solutions on modern hardware and software to ensure credentials are securely stored.
  - Ensure storage of clear text passwords in Local Security Authority Subsystem Service (LSASS) memory is disabled. **Note:** for Windows 8, this is enabled by default. For more information see Microsoft Security Advisory Update to Improve Credentials Protection and Management(link is external).
  - Consider disabling or limiting NTLM and WDigest Authentication.
  - Implement Credential Guard for Windows 10 and Server 2016 (refer to Microsoft: Manage Windows Defender Credential Guard for more information). For Windows Server 2012R2, enable Protected Process Light for Local Security Authority (LSA).
  - Minimize the Active Directory (AD) attack surface to reduce malicious ticket-granting activity. Malicious activity such as “Kerberoasting” takes advantage of Kerberos’ Ticket Granting Service (TGS) and can be used to obtain hashed credentials that malicious cyber actors attempt to crack.
- Audit domain controllers to log successful Kerberos TGS requests and ensure the events are monitored for anomalous activity.
  - Secure accounts.
  - Enforce the principle of least privilege. Administrator accounts should have the minimum permission necessary to complete their tasks.
  - Ensure there are unique and distinct administrative accounts for each set of administrative tasks.
  - Create non-privileged accounts for privileged users and ensure they use the non-privileged accounts for all non-privileged access (e.g., web browsing, email access).
- Disable inactive accounts uniformly across the AD, MFA systems, etc.
- Implement time-based access for privileged accounts. The FBI and CISA observed cybercriminals conducting increasingly impactful attacks against U.S. entities on holidays and weekends in 2021. Threat actors may view holidays and weekends—when offices are normally closed—as attractive timeframes, as there are fewer network defenders and IT support personnel at victim organizations. The just-in-time access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the zero-trust model) by setting network-wide policy to automatically disable admin accounts at the AD level. As needed, individual users can submit requests through an automated process that enables access to a system for a set timeframe.

Protective Controls and Architecture

- Identify, detect, and investigate abnormal activity that may indicate lateral movement by a threat actor, ransomware, or other malware. Use network monitoring tools and host-based logs and

monitoring tools, such as an endpoint detection and response (EDR) tool. EDR tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- Implement a firewall and configure it to block Domain Name System (DNS) responses from outside the enterprise network or drop Internet Control Message Protocol (ICMP) packets. Review which admin services need to be accessible externally and allow those explicitly, blocking all others by default.
  - U.S. Defense Industrial Base organizations may sign up for the NSA Cybersecurity Collaboration Center's Protective Domain Name System (PDNS) services.
- Enable web application firewalls to mitigate application-level DDoS attacks.
- Implement a multi-content delivery network (CDN) solution. This will minimize the threat of DDoS attacks by distributing and balancing web traffic across a network.

Vulnerability and Configuration Management

- Use an antivirus programs that uses heuristics and reputational ratings to check a file's prevalence and digital signature prior to execution. **Note:** organizations should assess the risks inherent in their software supply chain (including its security/antivirus software supply chain) in light of the existing threat landscape.
  - Set antivirus/antimalware programs to conduct regular scans of IT network assets using up-to-date signatures.
  - Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.
- Implement rigorous configuration management programs. Ensure the programs can track and mitigate emerging threats. Review system configurations for misconfigurations and security weaknesses.
- Disable all unnecessary ports and protocols.
  - Review network security device logs and determine whether to shut off unnecessary ports and protocols. Monitor common ports and protocols for command and control activity.
  - Turn off or disable any unnecessary services (e.g., PowerShell) or functionality within devices.
- Identify business-to-business VPNs and block high-risk protocols.
- Ensure OT hardware is in read-only mode.
- Enable strong spam filters.
  - Enable strong spam filters to prevent phishing emails from reaching end users.
  - Filter emails containing executable files to prevent them from reaching end users.
  - Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments.
- Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary and remove or disable outdated versions of SMB (i.e., SMB version 1). Threat actors use SMB to propagate malware across organizations.
- Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
- Implement listing policies for applications and remote access that only allow systems to execute

known and permitted programs under an established security policy.
- Open document readers in protected viewing modes to help prevent active content from running.

Responding to Cyber Incidents

U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities urge network defenders of critical infrastructure organizations to exercise due diligence in identifying indicators of malicious activity. Organizations detecting potential APT or ransomware activity in their IT or OT networks should:

1. Immediately isolate affected systems.
2. For DDoS attacks:
   a. Identify the source address originating the attack via the SIEM or logging service. If the attack is originating from a single pool of IP addresses, block IP traffic from suspected IPs via access control lists or by contacting your internet service provider (ISP).
   b. Enable firewall rate limiting to restrict the amount of IP traffic coming in from suspected IP addresses
   c. Notify your ISP and enable remote triggered blackhole (RTBH).
3. Secure backups. Ensure your backup data is offline and secure. If possible, scan your backup data with an antivirus program to ensure it is free of malware.
4. Collect and review relevant logs, data, and artifacts.
5. Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
6. Report incidents to appropriate cyber and law enforcement authorities:

- **U.S organizations:** share information about incidents and anomalous activity to CISA's 24/7 Operations Center at report@cisa.gov(link sends email) or (888) 282-0870 and/or the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov(link sends email). For ransomware incidents, organizations can also report to the U.S. Secret Service via a U.S. Secret Service Field Office.
- **Australian organizations:** if you have questions about this advice or have indications that your environment has been compromised, call the ACSC at 1300 CYBER1 (1300 292 371). To report an incident see cyber.gov.au/acsc/report.
- **Canadian organizations:** report incidents by emailing CCCS at contact@cyber.gc.ca(link sends email).
- **New Zealand organizations**: if your organization requires assistance from the National Cyber Security Centre, contact them directly via telephone at (04) 498-7654 or via email at ncscincidents@ncsc.govt.nz(link sends email).
- **UK organizations:** report a significant cybersecurity incident at ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

For additional guidance on responding to a ransomware incident, see the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.

See the joint advisory from Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity for guidance on

hunting or investigating a network, and for common mistakes in incident handling.

Additionally, CISA, the FBI, and NSA encourage U.S. critical infrastructure owners and operators to see CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to federal civilian branch agencies, these playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail each step for both incident and vulnerability response.

Note: U.S., Australian, Canadian, New Zealand, and UK cyber authorities strongly discourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom does not guarantee that a victim's files will be recovered.

RESOURCES

- For more general information on Russian state-sponsored malicious cyber activity, see CISA's Russia Cyber Threat Overview and Advisories webpage and joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure.
- For alerts on malicious and criminal cyber activity, see the FBI Internet Crime Complaint Center webpage.
- For more information and resources on protecting against and responding to ransomware, refer to StopRansomware.gov, a centralized, U.S. government webpage providing ransomware resources and alerts.
- For more information on mitigating DDoS attacks, see NCSC-UK Denial of Service (DoS) Guidance.
- For more information on managing cybersecurity incidents, see NZ NCSC Incident Management: Be Resilient, Be Prepared.
- For information on destructive malware, see joint CSA Destructive Malware Targeting Organizations in Ukraine.
- Critical infrastructure owners and operators with OT/ICS networks, should review the following resources for additional information:
  - Joint CSA NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems
  - CISA factsheet Rising Ransomware Threat to Operational Technology Assets

DISCLAIMER

The information you have accessed or received is being provided "as is" for informational purposes only. CISA, NSA, FBI, ACSC, CCCS, NZ NCSC, NCSC-UK, and the UK National Crime Agency (NCA) do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring.

TRADEMARK RECOGNITION

MITRE and ATT&CK are registered trademarks of The MITRE Corporation. Kubernetes is a

registered trademark of The Linux Foundation.

PURPOSE

This document was developed by U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

REFERENCES

[1] Cybersecurity and Infrastructure Security Agency
[2] Federal Bureau of Investigation
[3] National Security Agency
[4] Australian Cyber Security Centre
[5] Canadian Centre for Cyber Security(link is external)
[6] New Zealand's National Cyber Security Centre
[7] United Kingdom's National Cyber Security Centre
[8] United Kingdom's National Crime Agency
[9] U.S. DOJ Press Release: U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts
[10] U.S. DOJ Press Release: Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide
[11] CrowdStrike Blog: Early Bird Catches the Wormhole: Observations from the StellarParticle Campaign(link is external)
[12] U.S. White House Statement: FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian
[13] Government of Canada Statement on SolarWinds Cyber Compromise(link is external)
[14] UK Government Press Release: Russia: UK and US expose global campaign of malign activity by Russian intelligence services
[15] MITRE ATT&CK: APT29
[16] Joint CSA Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware
[17] Joint CSA Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments
[18] MITRE ATT&CK APT28
[19] Joint CSA New Sandworm Malware Cyclops Blink Replaces VPNFilter
[20] UK Government Press Release: UK condemns Russia's GRU over Georgia cyber-attacks
[21] U.S. Department of State, Press Statement: The United States Condemns Russian Cyber Attack Against the Country of Georgia
[22] Government of Canada CSE Statement on Malicious Russian Cyber Activity Targeting Georgia(link is external)
[23] UK Government Press Release: UK condemns Russia's GRU over Georgia cyber-attacks
[24] MITRE ATT&CK The Sandworm Team
[25] U.S. Department of the Treasury Press Release: Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware
[26] UK Government Press Release: UK exposes Russian spy agency behind cyber incident

[27] U.S. DOJ Press Release: Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide
[28] MITRE ATT&CK TEMP.Veles
[29] NSA and NCSC-UK Cybersecurity Advisory Turla Group Exploits Iranian APT To Expand Coverage Of Victims
[30] CrowdStrike Adversary Profile: VENEMOUS BEAR(link is external)
[31] KELA Cybersecurity Intelligence Center: Ain't No Actor Trustworthy Enough: The importance of validating sources(link is external)
[32] Twitter: Valery Marchive Status, Feb. 25, 2022 1:41 PM(link is external)
[33] The Record by Recorded Future: Russia or Ukraine: Hacking Groups Take Sides(link is external)
[34] Twitter: CyberKnow Status, March 29, 2022, 7:54 AM(link is external)
[35] CrowdStrike Blog: Who is Salty Spider (Sality)?(link is external)
[36] Proofpoint Blog: New Year, New Version of DanaBot(link is external)
[37] Zscaler Blog: Spike in DanaBot Malware Activity(link is external)
[38] Proofpoint Blog: New Year, New Version of DanaBot(link is external)
[39] The Record by Recorded Future: Russia or Ukraine: Hacking Groups Take Sides(link is external)
[40] TechTarget: Conti ransomware gang backs Russia, threatens US(link is external)
[41] The Record by Recorded Future: Russia or Ukraine: Hacking Groups Take Sides(link is external)

ACKNOWLEDGEMENTS

The U.S., Australian, Canadian, New Zealand, and UK cyber authorities would like to thank CrowdStrike, Google, LookingGlass Cyber, Mandiant, Microsoft, and Secureworks for their contributions to this CSA.

Contact Information

U.S. organizations: to report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact CISA's 24/7 Operations Center at report@cisa.gov(link sends email) or (888) 282-0870 and/or to the FBI via your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by email at CyWatch@fbi.gov(link sends email). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact the Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov(link sends email). **Australian organizations:** visit cyber.gov.au/acsc/report or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories. **Canadian organizations:** report incidents by emailing CCCS at contact@cyber.gc.ca(link sends email). **New Zealand organizations:** report cyber security incidents to ncscincidents@ncsc.govt.nz(link sends email) or call 04 498 7654. **United Kingdom organizations:** report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

Revisions

April 20, 2022: Initial version

Contact Us

(888)282-0870

Send us email(link sends email)

Download PGP/GPG keys

Submit website feedback

Subscribe to Alerts

Receive security alerts, tips, and other updates.

Enter your email address

Sign Up

HSIN

Report

RANSOMWARE GUIDE

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased, with some demands exceeding US $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

On September 30, 2020, a joint Ransomware Guide was released, which is a customer centered, one-stop resource with best practices and ways to prevent, protect and/or respond to a ransomware attack. CISA and MS-ISAC are distributing this guide to inform and enhance network defense and reduce exposure to a ransomware attack:

This Ransomware Guide includes two resources:

- **Part 1: Ransomware Prevention Best Practices**
- **Part 2: Ransomware Response Checklist**

CISA recommends that organizations take the following initial steps:

- Join an information sharing organization, such as one of the following:
  - Multi-State Information Sharing and Analysis Center (MS-ISAC): https://learn.cisecurity.org/ms-isac-registration
  - Election Infrastructure Information Sharing and Analysis Center (EI-ISAC): https://learn.cisecurity.org/ei-isac-registration
  - Sector-based ISACs - National Council of ISACs: https://www.nationalisacs.org/member-isacs
  - Information Sharing and Analysis Organization (ISAO) Standards Organization: https://www.isao.org/information-sharing-groups/
- Engage CISA to build a lasting partnership and collaborate on information sharing, best practices, assessments, exercises, and more:
  - SLTT organizations: CyberLiaison_SLTT@cisa.dhs.gov
  - Private sector organizations: CyberLiaison_Industry@cisa.dhs.gov
- Engaging with your ISAC, ISAO, and with CISA will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.

Ransomware Guide (Sept. 2020)

Expand All Sections

TLP:WHITE

Part 1: Ransomware Prevention Best Practices

Be Prepared

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
  - Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
  - Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
    - Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
  - In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
  - Review available incident response guidance, such as the Public Power Cyber Incident Response Playbook (https://www.publicpower. org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf), a resource and guide to:
    - Help your organization better organize around cyber incident response, and
    - Develop a cyber incident response plan.
  - The Ransomware Response Checklist, which forms the other half of this Ransomware Guide, serves as an adaptable, ransomware-specific annex to organizational cyber incident response or disruption plans.

Ransomware Infection Vector: Internet-Facing Vulnerabilities and Misconfigurations

- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.
  - CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: https://www.cisa.gov/cyber-resource-hub.
- Regularly patch and update software and OSs to the latest available versions.
  - Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins, and document readers—for known vulnerabilities.
- Ensure devices are properly configured and that security features are enabled. For example, disable ports and protocols that are not being used for a business purpose (e.g., Remote Desktop Protocol [RDP] – Transmission Control Protocol [TCP] Port 3389).
- Employ best practices for use of RDP and other remote desktop services. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later propagate ransomware. See CISA Alert AA20-073A, Enterprise VPN Security (https://us-cert.cisa.gov/ncas/alerts/aa20-073a).
  - Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multi-factor authentication (MFA), and log RDP login attempts.
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Based on this specific threat, organizations should consider the following actions to protect their networks:

- Disable SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on th existing systems or applications) that may break when disabled.
  - Remove dependencies through upgrades and reconfiguration: Upgrade to SMBv3 (or most current version) along with SMB signing.
- Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.

Ransomware Infection Vector: Phishing

- Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.
- Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall.
- To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification. DMARC builds on the widely deployed sender policy framework and Domain Keys Identified Mail protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email.
- Consider disabling macro scripts for Microsoft Office files transmitted via email. These macros can be used to deliver ransomware.

Ransomware Infection Vector: Precursor Malware Infection

- Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions. CISA recommends using a centrally managed antivirus solution. This enables detection of both “precursor” malware and ransomware.
  - A ransomware infection may be evidence of a previous, unresolved network compromise. For example, many ransomware infections are the result of existing malware infections, such as TrickBot, Dridex, or Emotet.
  - In some cases, ransomware deployment is just the last step in a network compromise and is dropped as a way to obfuscate previous post-compromise activities.
- Use application directory allowlisting on all assets to ensure that only authorized software can run, and all unauthorized software is blocked from executing.
  - Enable application directory allowlisting through Microsoft Software Restriction Policy or AppLocker.
  - Use directory allowlisting rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from PROGRAMFILES, PROGRAMFILES(X86), and SYSTEM32. Disallow all other locations unless an exception is granted.
- Consider implementing an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.

Ransomware Infection Vector: Third Parties and Managed Service Providers

- Take into consideration the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization relies on to meet its mission. MSPs have been an infection vector for ransomware impacting client organizations.
  - If a third party or MSP is responsible for maintaining and securing your organization’s backups, ensure they are following the applicable best practices outlined above. Using contract language to formalize your security requirements is a best practice.
- Understand that adversaries may exploit the trusted relationships your organization has with third parties and MSPs. See CISA’s APTs Targeting IT Service Provider Customers (https:// us-cert.cisa.gov/APTs-Targeting-IT-Service-Provider-Customers).
  - Adversaries may target MSPs with the goal of compromising MSP client organizations; they may use MSP network connections and access to client organizations as a key vector to propagate malware and ransomware.

- Adversaries may spoof the identity of—or use compromised email accounts associated with—entities you has a trusted relationship with in order to phish your users, enabling network compromise and disclosure of information.

General Best Practices and Hardening Guidance

- Employ MFA for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
  - If you are using passwords, use strong passwords (https://us-cert.cisa.gov/ncas/tips/ST04-002) and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts. Password managers can help you develop and manage secure passwords.
- Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs. Threat actors often seek out privileged accounts to leverage to help saturate networks with ransomware.
  - Restrict user permissions to install and run software applications.
  - Limit the ability of a local administrator account to log in from a local interactive session (e.g., "Deny access to this computer from the network.") and prevent access via an RDP session.
  - Remove unnecessary accounts and groups and restrict root access.
  - Control and limit local administration.
  - Make use of the Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.
  - Audit user accounts regularly, particularly Remote Monitoring and Management accounts that are publicly accessible—this includes audits of third-party access given to MSPs.
- Leverage best practices and enable security settings in association with cloud environments, such as Microsoft Office 365 (https://www.us-cert.cisa.gov/ncas/alerts/aa20-120a).
- Develop and regularly update a comprehensive network diagram that describes systems and data flows within your organization's network (see figure 1). This is useful in steady state and can help incident responders understand where to focus their efforts.
  - The diagram should include depictions of covered major networks, any specific IP addressing schemes, and the general network topology (including network connections, interdependencies, and access granted to third parties or MSPs).
- Employ logical or physical means of network segmentation to separate various business unit or departmental IT resources within your organization as well as to maintain separation between IT and operational technology. This will help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors. See figures 2 and 3 for depictions of a flat (unsegmented) network and of a best practice segmented network.
  - Network segmentation can be rendered ineffective if it is breached through user error or non-adherence to organizational policies (e.g., connecting removable storage media or other devices to multiple segments).

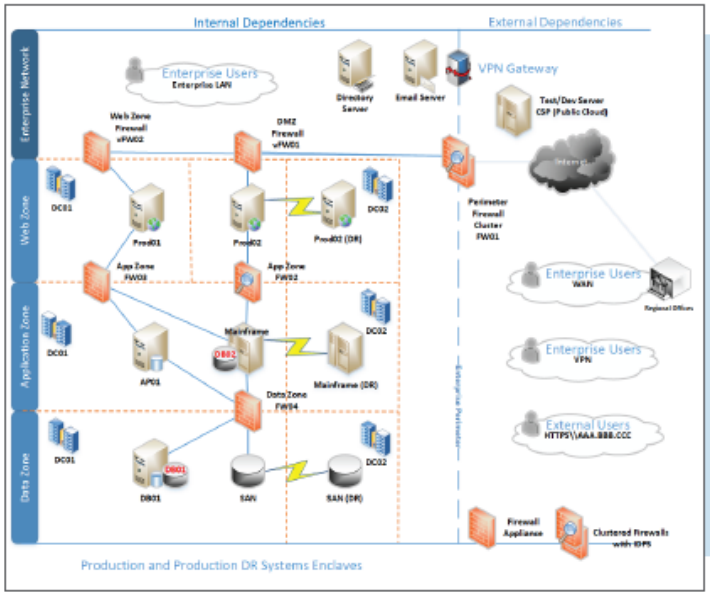


Figure 1. Example Network Diagram

- Ensure your organization has a comprehensive asset management approach.
  - Understand and inventory your organization's IT assets, both logical (e.g., data, software) and physical (e.g., hardware).
  - Understand which data or systems are most critical for health and safety, revenue generation, or other critical services, as well as any associated interdependencies (i.e., "critical asset or system list"). This will aid your organization in determining restoration priorities should an incident occur. Apply more comprehensive security controls or safeguards to critical assets. This requires organization-wide coordination.
  - Use the MS-ISAC Hardware and Software Asset Tracking Spreadsheet: https://www.cisecurity. org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/.
- Restrict usage of PowerShell, using Group Policy, to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows OSs should be permitted to use PowerShell. Update PowerShell and enable enhanced logging. PowerShell is a cross-platform, command-line, shell and scripting language that is a component of Microsoft Windows. Threat actors use PowerShell to deploy ransomware and hide their malicious activities.
  - Update PowerShell instances to version 5.0 or later and uninstall all earlier PowerShell versions. Logs from PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities.
    - PowerShell logs contain valuable data, including historical OS and registry interaction and possible tactics, techniques, and procedures of a threat actor's PowerShell use.
  - Ensure PowerShell instances (use most current version) have module, script block, and transcription logging enabled (enhanced logging).
    - The two logs that record PowerShell activity are the "PowerShell" Windows Event Log and the "PowerShell Operational" Log. CISA recommends turning on these two Windows Event Logs with a retention period of 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.

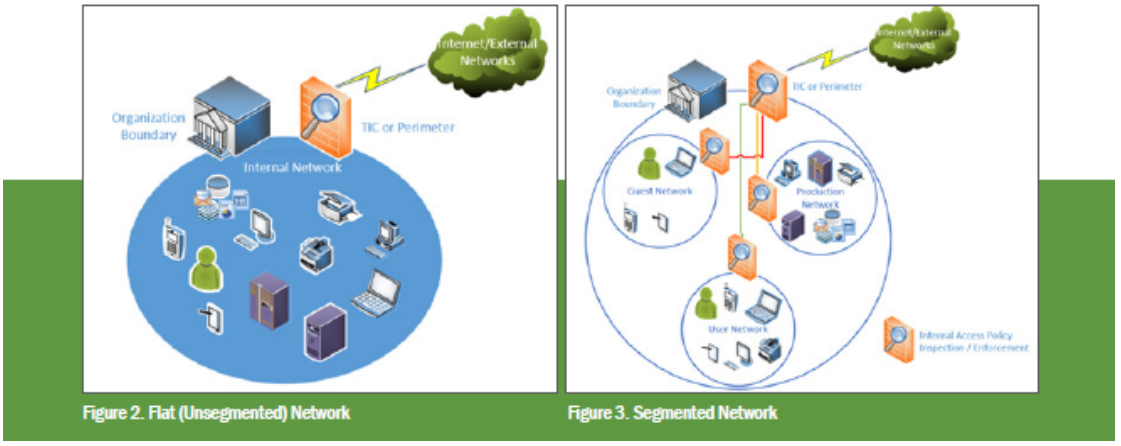


Figure 2. Flat (Unsegmented) Network Figure 3. Segmented Network

- Secure domain controllers (DCs). Threat actors often target and use DCs as a staging point to spread ransomware network-wide.
  - The following list contains high-level suggestions on how best to secure a DC:
    - Ensure that DCs are regularly patched. This includes the application of critical patches as soon as possible.
    - Ensure the most current version of the Windows Server OS is being used on DCs. Security features are better integrated in newer versions of Windows Server OSs, including Active Directory security features. Use Active Directory configuration guides, such as those available from Microsoft (https://docs.microsoft.com/ en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-forsecuring-active-directory), when configuring available security features.
    - Ensure that no additional software or agents are installed on DCs, as these can be leveraged to run arbitrary code on the system.
    - Access to DCs should be restricted to the Administrators group. Users within this group should be limited and have separate accounts used for day-to-day operations with non-administrative permissions.
    - DC host firewalls should be configured to prevent internet access. Usually, these systems do not have a valid need for direct internet access. Update servers with internet connectivity can be used to pull necessary updates

allowing internet access for DCs.

- CISA recommends the following DC Group Policy settings:
  (Note: This is not an all-inclusive list and further steps should be taken to secure DCs within the environment.)
  - The Kerberos default protocol is recommended for authentication, but if it is not used, enable NTLM auditing to ensure that only NTLMv2 responses are being sent across the network. Measures should be taken to ensure that LM and NTLM responses are refused, if possible.
  - Enable additional protections for Local Security Authentication to prevent code injection capable of acquiring credentials from the system. Prior to enabling these protections, run audits against the lsass.exe program to ensure an understanding of the programs that will be affected by the enabling of this protection.
  - Ensure that SMB signing is required between the hosts and the DCs to prevent the use of replay attacks on the network. SMB signing should be enforced throughout the entire domain as an added protection against these attacks elsewhere in the environment.
- Retain and adequately secure logs from both network devices and local hosts. This supports triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain whether an incident has occurred.
  9
  - Set up centralized log management using a security information and event management tool. This enables an organization to correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact to the organization as a whole.
  - Maintain and back up logs for critical systems for a minimum of one year, if possible.

- Baseline and analyze network activity over a period of months to determine behavioral patterns so that normal, legitimate activity can be more easily distinguished from anomalous network activity (e.g., normal vs anomalous account activity).
  - Business transaction logging—such as logging activity related to specific or critical applications—is another useful source of information for behavioral analytics.

Contact CISA for These No-Cost Resources

- Information sharing with CISA and MS-ISAC (for SLTT organizations) includes bi-directional sharing of best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware
- Policy-oriented or technical assessments help organizations understand how they can improve their defenses to avoid ransomware infection: https://www.cisa.gov/cyber-resource-hub
  - Assessments include Vulnerability Scanning and Phishing Campaign Assessment
- Cyber exercises evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario
- CISA Cybersecurity Advisors (CSAs) advise on best practices and connect you with CISA resources to manage cyber risk
- Contacts:
  - SLTT organizations: CyberLiaison_SLTT@cisa.dhs.gov
  - Private sector organizations: CyberLiaison_Industry@cisa.dhs.gov

Ransomware Quick References

- Ransomware: What It Is and What to Do About It (CISA): General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One -Pager_and_Technical_Document-FINAL.pdf
- Ransomware (CISA): Introduction to ransomware, notable links to CISA products on protecting networks, specific ransomware threats, and other resources: https://www.us-cert.cisa.gov/ransomware
- Security Primer – Ransomware (MS-ISAC): Outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations: https://www.cisecurity.org/white-papers/security-primer-ransomware/
- Ransomware: Facts, Threats, and Countermeasures (MSISAC):
  Facts about ransomware, infection vectors, ransomware

capabilities, and how to mitigate the risk of ransomware infection: https://www.cisecurity.org/blog/ransomwarefacts-threats-and-countermeasures/

- Security Primer – Ryuk (MS-ISAC): Overview of Ryuk ransomware, a prevalent ransomware variant in the SLTT government sector, that includes information regarding preparedness steps organizations can take to guard against infection: https://www.cisecurity.org/white-papers/security-primer-ryuk/

Part 2: Ransomware Response Checklist

TLP:WHITE

FEDERAL BUREAU of INVESTIGATION

Internet Crime Report

2021

INTERNET CRIME COMPLAINT CENTER

Contents

INTRODUCTION

Dear Reader,

In 2021, America experienced an unprecedented increase in cyber attacks and malicious cyber activity. These cyber attacks compromised businesses in an extensive array of business sectors as well as the American public. As the cyber threat evolves and becomes increasingly intertwined with traditional foreign intelligence threats and emerging technologies, the FBI continues to leverage our unique authorities and partnerships to impose risks and consequences on our nation's cyber adversaries.

The FBI's Internet Crime Complaint Center (IC3) provides the American public with a direct outlet to report cyber crimes to the FBI. We analyze and investigate the reporting to track the trends and threats from cyber criminals and then share this data with our intelligence and law enforcement partners. The FBI, alongside our partners, recognizes how crucial information sharing of cyber activities is to prepare our partners to combat the cyber threat, through a whole-of-government approach. Critical to that approach is public reporting to IC3 - enabling us to fill in the missing pieces with this valuable information during the investigatory process. Not only does this reporting help to prevent additional crimes, it allows us to develop key insights on the ever-evolving trends and threats we face from malign cyber actors.

In 2021, IC3 continued to receive a record number of complaints from the American public: 847,376 reported complaints, which was a 7% increase from 2020, with potential losses exceeding $6.9 billion. Among the 2021 complaints received, ransomware, business e-mail compromise (BEC) schemes, and the criminal use of cryptocurrency are among the top incidents reported. In 2021, BEC schemes resulted in 19,954 complaints with an adjusted loss of nearly $2.4 billion.

IC3's commitment to cyber victims and partnerships allow for the continued success through programs such as the IC3's Recovery Asset Team (RAT). Established in 2018, RAT streamlines communications with financial institutions and FBI field offices to assist freezing of funds for victims. In 2021, the IC3's RAT initiated the Financial Fraud Kill Chain (FFKC) on 1,726 BEC complaints involving domestic to domestic transactions with potential losses of $443,448,237. A monetary hold was placed on approximately $329 million, which represents a 74% success rate.

In 2021, heightened attention was brought to the urgent need for more cyber incident reporting to the federal government. Cyber incidents are in fact crimes deserving of an investigation, leading to judicial repercussions for the perpetrators who commit them. Thank you to all those readers who reported crimes to IC3 throughout the year. Without this reporting, we could not be as effective in ensuring consequences are imposed on those perpetrating these attacks and our understanding of these threats would not be as robust. Please visit IC3.gov to access the latest information on criminal internet activity.

The FBI's Cyber Division is working harder than ever to protect the American public and to instill safety, security, and confidence in a digitally connected world. We encourage everyone to use IC3 and reach out to their local FBI field office to report malicious activity. Together we can continue to create a safer and more secure cyber landscape.

Paul Abbate
Deputy Director
Federal Bureau of Investigation

THE IC3

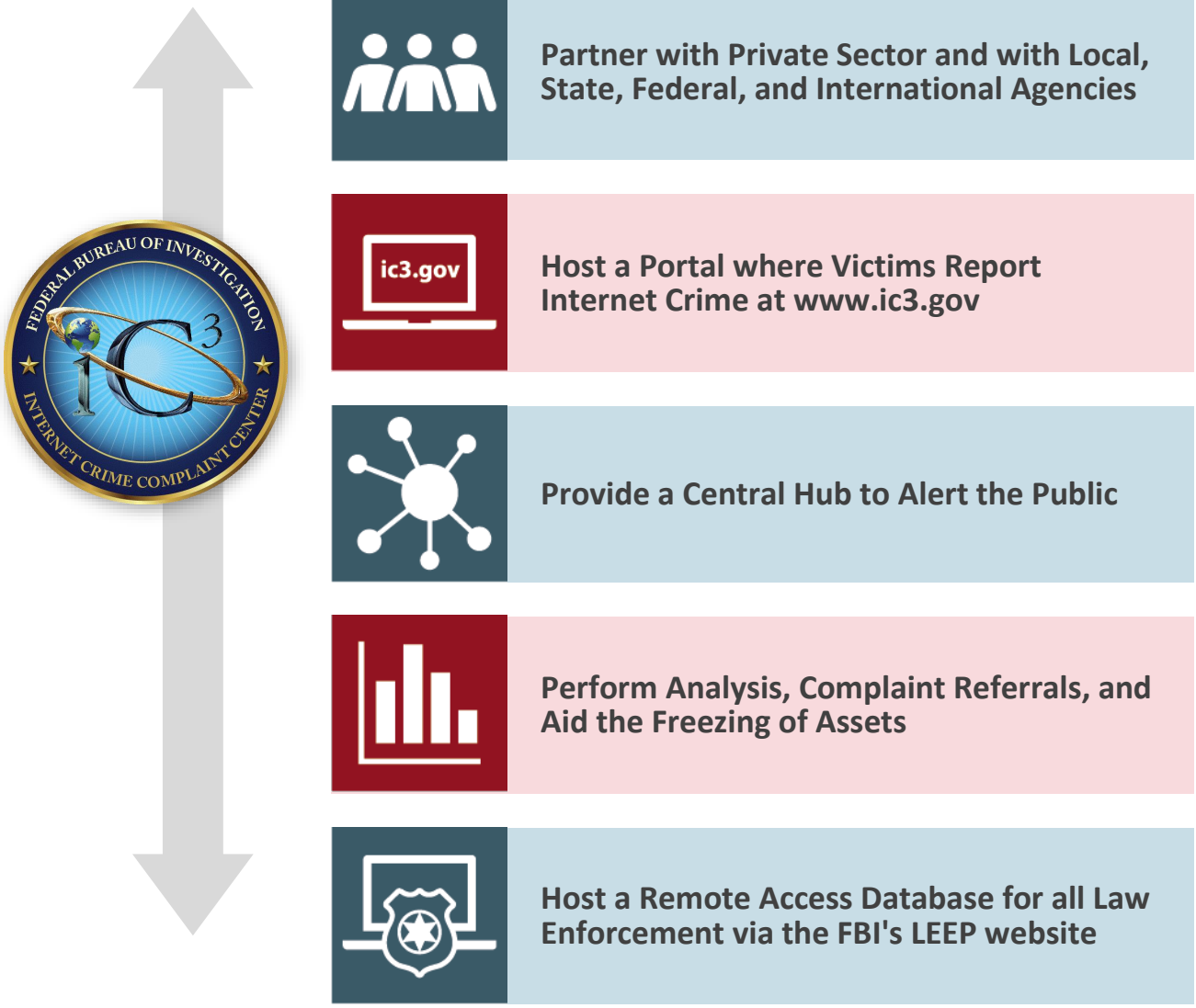
Today's FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities. We are focused on protecting the American people from terrorism, espionage, cyber attacks and major criminal threats, and on supporting our many partners with information, services, support, training, and leadership. The IC3 serves those needs as a mechanism to gather intelligence on cyber and internet crime so we can stay ahead of the threat.

The IC3 was established in May 2000 to receive complaints of internet related crime and has received more than 6.5 million complaints since its inception. Its mission is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected cyber enabled criminal activity, and to develop effective alliances with law enforcement and industry partners to help those who report. Information is analyzed and disseminated for investigative and intelligence purposes for law enforcement and for public awareness.

To promote public awareness, the IC3 aggregates the submitted data and produces an annual report to educate on the trends impacting the public. The quality of the data is directly attributable to the information ingested via the public interface, www.ic3.gov, and the data categorized based on the information provided in the individual complaints. The IC3 staff analyzes the data to identify trends in cyber crimes and how those trends may impact the public in the coming year.

THE IC3 ROLE IN COMBATING CYBER CRIME[1]

What we do



[1] Accessibility description: Image lists IC3's primary functions including partnering with private sector and with local, state, federal, and international agencies: hosting a victim reporting portal at www.ic3.gov; providing a central hub to alert the public to threats; Perform Analysis, Complaint Referrals, and Asset Recovery; and hosting a remote access database for all law enforcement via the FBI's LEEP website.

IC3 CORE FUNCTIONS[2]



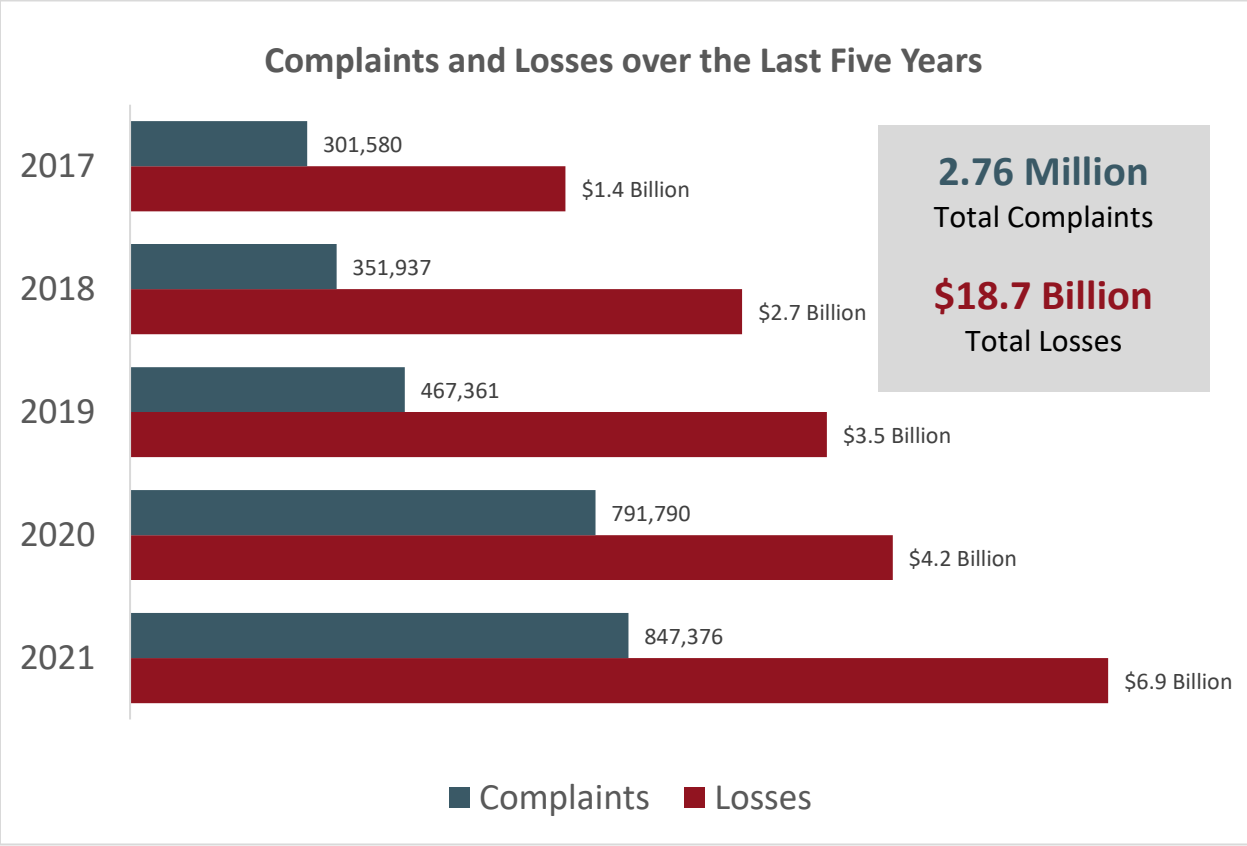

COLLECTION	ANALYSIS	PUBLIC AWARENESS	REFERRALS
The IC3 is the central point for Internet crime victims to report and alert the appropriate agencies to suspected criminal Internet activity. Victims are encouraged and often directed by law enforcement to file a complaint online at www.ic3.gov. Complainants are asked to document accurate and complete information related to Internet crime, as well as any other relevant information necessary to support the complaint.	The IC3 reviews and analyzes data submitted through its website to identify emerging threats and new trends. In addition, the IC3 quickly alerts financial Institutions to fraudulent transactions which enables the freezing of victim funds.	Public service announcements, industry alerts, and other publications outlining specific scams are posted to the www.ic3.gov website. As more people become aware of Internet crimes and the methods used to carry them out, potential victims are equipped with a broader understanding of the dangers associated with Internet activity and are in a better position to avoid falling prey to schemes online.	The IC3 aggregates related complaints to build referrals, which are forwarded to local, state, federal, and international law enforcement agencies for potential investigation. If law enforcement investigates and determines a crime has been committed, legal action may be brought against the perpetrator.

[2] Accessibility description: Image contains icons with the core functions. Core functions - Collection, Analysis, Public Awareness, and Referrals - are listed in individual blocks as components of an ongoing process.

IC3 COMPLAINT STATISTICS

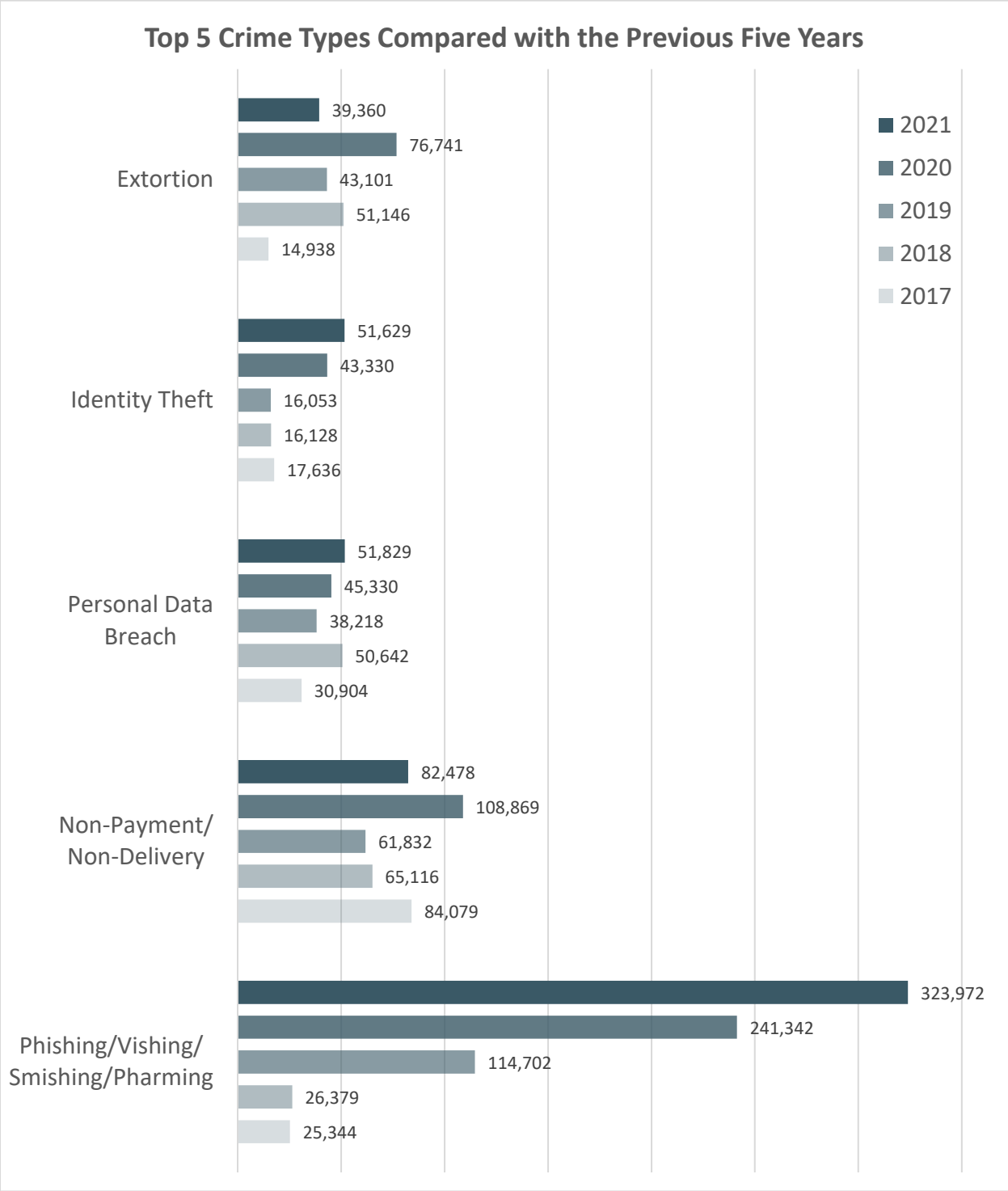
LAST 5 YEARS

Over the last five years, the IC3 has received an average of 552,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.[3]



[3] Accessibility description: Chart includes yearly and aggregate data for complaints and losses over the years 2017 to 2021. Over that time, IC3 received a total of 2,760,044 complaints, reporting a loss of $18.7 billion.

TOP 5 CRIME TYPE COMPARSON[4]



[4] Accessibility description: Chart includes a victim loss comparison for the top five reported crime types for the years of 2017 to 2021.

THREAT OVERVIEWS FOR 2021

BUSINESS EMAIL COMPROMISE (BEC)

In 2021, the IC3 received 19,954 Business Email Compromise (BEC)/ Email Account Compromise (EAC) complaints with adjusted losses at nearly $2.4 billion. BEC/EAC is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

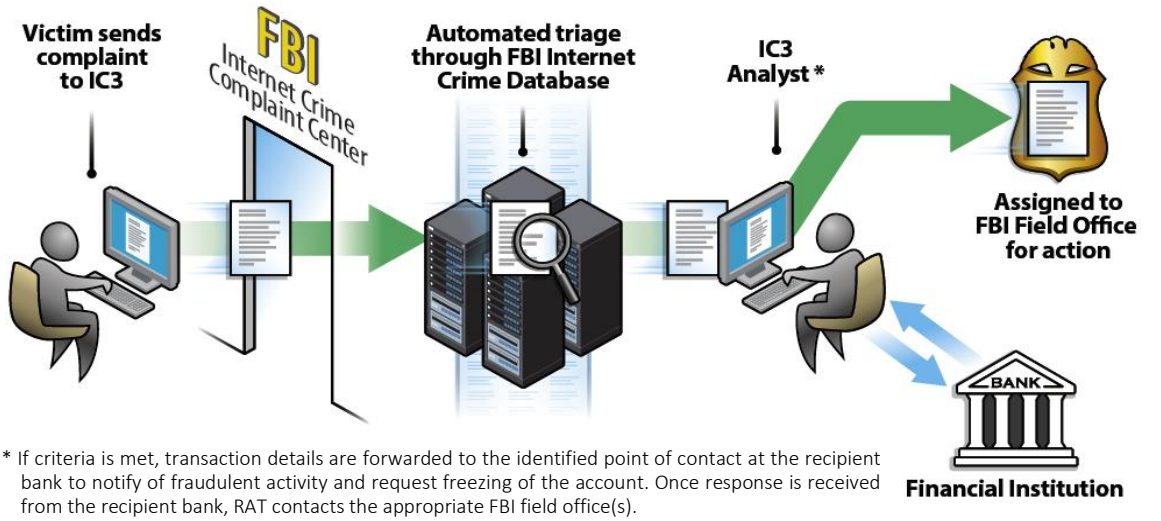
As fraudsters have become more sophisticated and preventative measures have been put in place, the BEC/EAC scheme has continually evolved in kind. The scheme has evolved from simple hacking or spoofing of business and personal email accounts and a request to send wire payments to fraudulent bank accounts. These schemes historically involved compromised vendor emails, requests for W-2 information, targeting of the real estate sector, and fraudulent requests for large amounts of gift cards. Now, fraudsters are using virtual meeting platforms to hack emails and spoof business leaders' credentials to initiate the fraudulent wire transfers. These fraudulent wire transfers are often immediately transferred to cryptocurrency wallets and quickly dispersed, making recovery efforts more difficult.

The COVID-19 pandemic and the restrictions on in-person meetings led to increases in telework or virtual communication practices. These work and communication practices continued into 2021, and the IC3 has observed an emergence of newer BEC/EAC schemes that exploit this reliance on virtual meetings to instruct victims to send fraudulent wire transfers. They do so by compromising an employer or financial director's email, such as a CEO or CFO, which would then be used to request employees to participate in virtual meeting platforms. In those meetings, the fraudster would insert a still picture of the CEO with no audio, or a "deep fake" audio through which fraudsters, acting as business executives, would then claim their audio/video was not working properly. The fraudsters would then use the virtual meeting platforms to directly instruct employees to initiate wire transfers or use the executives' compromised email to provide wiring instructions.

IC3 RECOVERY ASSET TEAM

The Internet Crime Complaint Center's Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for victims who made transfers to domestic accounts under fraudulent pretenses.

RAT Process[5]



* If criteria is met, transaction details are forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, RAT contacts the appropriate FBI field office(s).

The RAT functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis.

Goals of RAT-Financial Institution Partnership

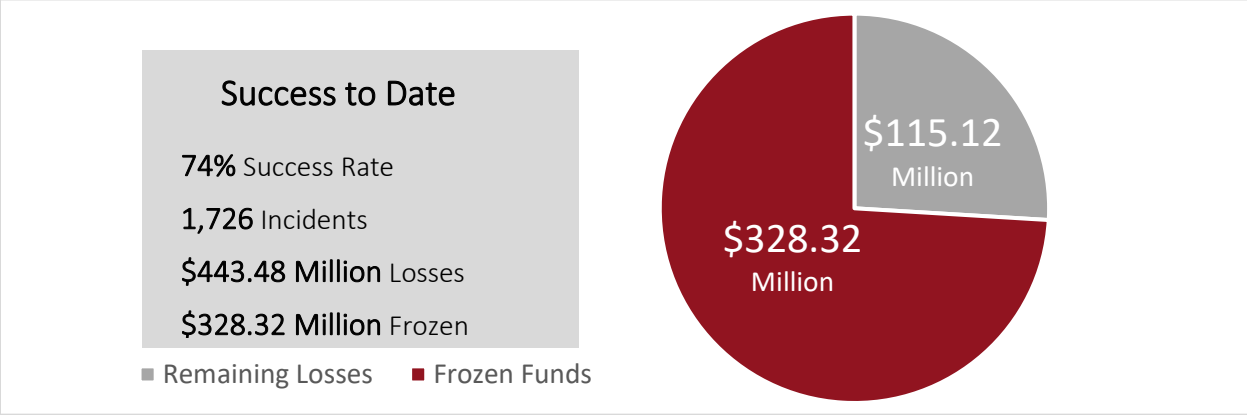
- Assist in the identification of potentially fraudulent accounts across the sector.
- Remain at the forefront of emerging trends among financial fraud schemes.
- Foster a symbiotic relationship in which information is appropriately shared.

Guidance for BEC Victims

- Contact the originating financial institution as soon as fraud is recognized to request a recall or reversal and a Hold Harmless Letter or Letter of Indemnity.
- File a detailed complaint with www.ic3.gov. It is vital the complaint contain all required data in provided fields, including banking information.
- Visit www.ic3.gov for updated PSAs regarding BEC trends as well as other fraud schemes targeting specific populations, like trends targeting real estate, pre-paid cards, and W-2s, for example.
- Never make any payment changes without verifying the change with the intended recipient; verify email addresses are accurate when checking email on a cell phone or other mobile device

[5] Accessibility description: Image shows the different stages of a complaint in the RAT process.

RAT SUCCESSES[6]



The IC3 RAT has proven to be a valuable resource for field offices and victims. The following are three examples of the RAT's successful contributions to investigative and recovery efforts:

Philadelphia

In December 2021, the IC3 received a complaint filed by a victim roadway commission regarding a wire transfer of more than $1.5 million to a fraudulent U.S. domestic bank account. The IC3 RAT quickly notified the recipient financial institution of the fraudulent account by initiating the financial fraud kill chain. Collaboration between the IC3 RAT, the recipient financial institution, and the Philadelphia Field office resulted in learning the subject quickly depleted the wired funds from the original account into two separate accounts held at the same institution. The financial institution was able to quickly identify the second-hop accounts and freeze the funds, making a full recovery possible.

Memphis

In June 2021, the IC3 received a complaint filed by a victim law office regarding a wire transfer of more than $198k to a fraudulent U.S. domestic account. IC3 RAT collaboration with the Memphis Field Office and the recipient financial institution resulted in learning the domestic account was a correspondent account for a fraudulent account in Nigeria. IC3 RAT immediately initiated the international FFKC to FinCEN and LEGAT Abuja, which resulted in freezing the full wired amount. The victim forwarded a note of gratitude for all the work put into their case.

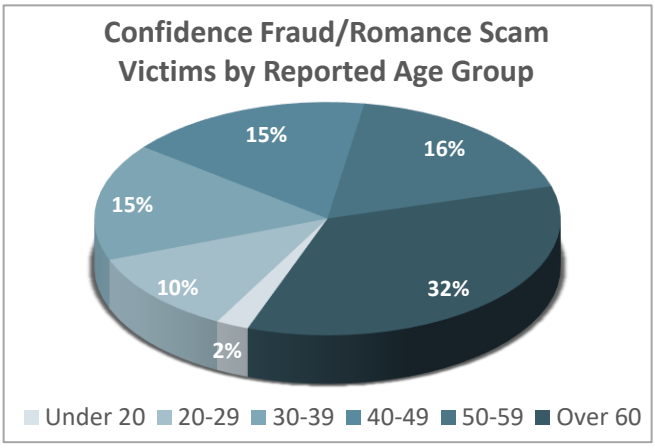
Albany

In October 2021, the IC3 received a complaint filed by a victim of a tech support scam where an unauthorized wire transfer of $53k was sent from their account to a U.S. domestic custodial account held by a cryptocurrency exchange (CE). The IC3 RAT immediately notified the recipient financial institution and collaborated with the CE that held the account. With the knowledge that funds sent to cryptocurrency accounts will be depleted to crypto faster than the usual wire transfer gets depleted, the immediate efforts of initiating the financial fraud kill chain with the CE resulted in the freezing of the funds in the custodial account before they could be depleted to purchase or withdraw cryptocurrency. Further collaboration with the domestic financial institution and the Albany Field Office confirmed the funds were frozen in the account, making a full recovery possible.

[6] Accessibility description: Image shows Success to Date to include 74% Success Rate; 1,726 Incidents; $433.48 Million in Losses; and $328.32. Million Frozen.

CONFIDENCE FRAUD / ROMANCE SCAMS[7]

Confidence Fraud/Romance scams encompass those designed to pull on a victim's "heartstrings." In 2021, the IC3 received reports from 24,299 victims who experienced more than $956 million in losses to Confidence Fraud/Romance scams. This type of fraud accounts for the third highest losses reported by victims.



Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and confidence. The scammer uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim. The criminals who carry out Romance scams are experts at what they do and will seem genuine, caring, and believable. The scammer's intention is to quickly establish a relationship, endear himself/herself to the victim, gain trust, and eventually ask for money. Scammers may propose marriage and make plans to meet in person, but that will never happen. Scam artists often say they are in the military, or a trades-based industry engaged in projects outside the U.S. That makes it easier to avoid meeting in person—and more plausible when they request money be sent overseas for a medical emergency or unexpected legal fee. Grandparent Scams also fall into this category, where criminals impersonate a panicked loved one, usually a grandchild, nephew, or niece of an elderly person. The loved one claims to be in trouble and needs money immediately.

Con artists are present on most dating and social media sites. In 2021, the IC3 received thousands of complaints from victims of online relationships resulting in sextortion or investment scams.

- Sextortion occurs when someone threatens to distribute your private and sensitive material if their demands are not met. In 2021, the IC3 received more than 18,000 sextortion-related complaints, with losses over $13.6 million. Please see the September 2021 IC3 PSA on Sextortion for more information.[8]
- Many victims of Romance scams also report being pressured into investment opportunities, especially using cryptocurrency. In 2021, the IC3 received more than 4,325 complaints, with losses over $429 million, from Confidence Fraud/Romance scam victims who also reported the use of investments and cryptocurrencies, or "pig butchering" –so named because victims' investment accounts are fattened up before draining, much a like a pig before slaughter. Additional information on "pig butchering" can be found in the September 2021 IC3 PSA I-091621-PSA.[9]

[7] Accessibility description: Chart shows Confidence Fraud/Romance Scam Victim by Reported Age Group. Under 20 2%; 20-29 10%; 30-39 15%; 40-49 15%; 50-59 16%; Over 60 32%

[8] FBI Warns about an Increase in Sextortion Complaints. https://www.ic3.gov/Media/Y2021/PSA210902

[9] Scammers Defraud Victims of Millions of Dollars in New Trend in Romance Scams.

CRYPTOCURRENCY (VIRTUAL CURRENCY)

In 2021, the IC3 received 34,202 complaints involving the use of some type of cryptocurrency, such as Bitcoin, Ethereum, Litecoin, or Ripple. While that number showed a decrease from 2020's victim count (35,229), the loss amount reported in IC3 complaints increased nearly seven-fold, from 2020's reported amount of $246,212,432, to total reported losses in 2021 of more than $1.6 billion.

Initially worth only fractions of pennies on the dollar, several cryptocurrencies have seen their values increase substantially, sometimes exponentially. Once limited to hackers, ransomware groups, and other denizens of the "dark web," cryptocurrency is becoming the preferred payment method for all types of scams – SIM swaps, tech support fraud, employment schemes, romance scams, even some auction fraud. It is extremely pervasive in investment scams, where losses can reach into the hundreds of thousands of dollars per victim. The IC3 has noted the following scams particularly using cryptocurrencies.

- Cryptocurrency ATMs: Automated Teller Machines (ATMs) used to purchase cryptocurrency are popping up everywhere. Regulations on the machines are lax and purchases are almost instantaneous and irreversible, making this payment method lucrative to criminals. In 2021, the IC3 received more than 1,500 reports of scams using crypto ATMs, with losses of approximately $28 million. The most common scams reported were Confidence Fraud/Romance, Investment, Employment, and Government Impersonation. Read more about crypto ATM scams in IC3 PSA I-110421-PSA.10
- Cryptocurrency support impersonators: Increasingly, crypto owners are falling victim to scammers impersonating support or security from cryptocurrency exchanges. Owners are alerted of an issue with their crypto wallet and are convinced to either give access to their crypto wallet or transfer the contents of their wallet to another wallet to "safeguard" the contents. Crypto owners are also searching online for support with their cryptocurrencies. Owners contact fake support numbers located online and are convinced to give up login information or control of their crypto accounts.
- Many victims of Romance scams also report being pressured into investment opportunities, especially using cryptocurrency. In 2021, the IC3 received more than 4,325 complaints, with losses over $429 million, from Confidence Fraud/Romance scam victims who also reported the use of investments and cryptocurrencies, or "pig butchering." The scammer's initial contact is typically made via dating apps and other social media sites. The scammer gains the confidence and trust of the victim, and then claims to have knowledge of cryptocurrency investment or trading opportunities that will result in substantial profits.

https://www.ic3.gov/Media/Y2021/PSA210916

[10] The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment https://www.ic3.gov/Media/Y2021/PSA211104

RANSOMWARE[11]

In 2021, the IC3 received 3,729 complaints identified as ransomware with adjusted losses of more than $49.2 million. Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.

Ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally. Although cyber criminals use a variety of techniques to infect victims with ransomware, phishing emails, Remote Desktop Protocol (RDP) exploitation, and exploitation of software vulnerabilities remained the top three initial infection vectors for ransomware incidents reported to the IC3. Once a ransomware threat actor has gained code execution on a device or network access, they can deploy ransomware. Note: these infection vectors likely remain popular because of the increased use of remote work and schooling starting in 2020 and continuing through 2021. This increase expanded the remote attack surface and left network defenders struggling to keep pace with routine software patching.[12]

Immediate Actions You Can Take Now to Protect Against Ransomware:

- Update your operating system and software.
- Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.
- If you use Remote Desktop Protocol (RDP), secure and monitor it.
- Make an offline backup of your data.

Ransomware and Critical Infrastructure Sectors

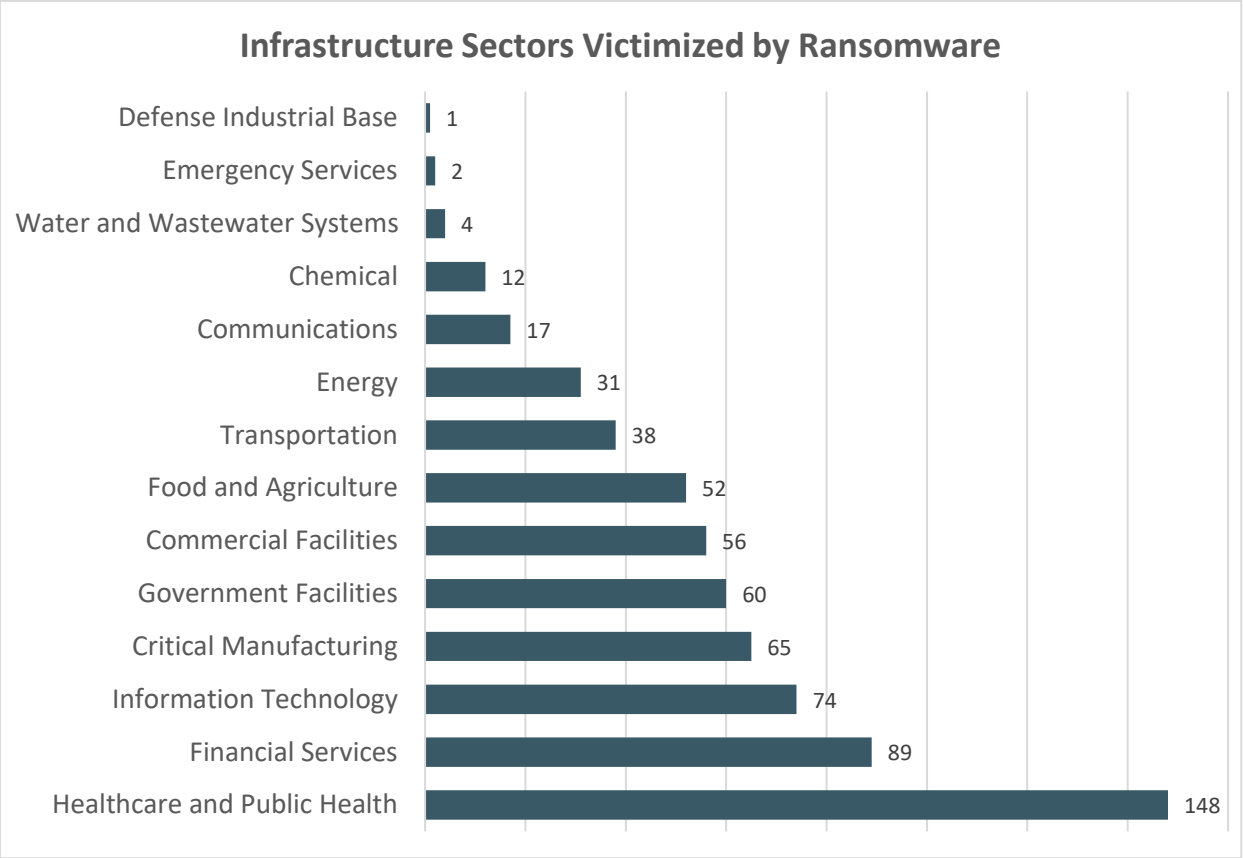
In June 2021, the IC3 began tracking reported ransomware incidents in which the victim was a member of a critical infrastructure sector. There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on our security, national economy, public health or safety, or any combination thereof.

[11] Accessibility description: Image shows actions you can Take to Protect Against Ransomware: Update your operating system. Implement user training and phishing exercises to raise awareness, secure and monitor Remote Desktop Protocol (DDP) if used, and make an offline backup of our data.

[12] 2021 Trends Show Increased Globalized Threat of Ransomware. https://www.ic3.gov/Media/News/2022/220209.pdf

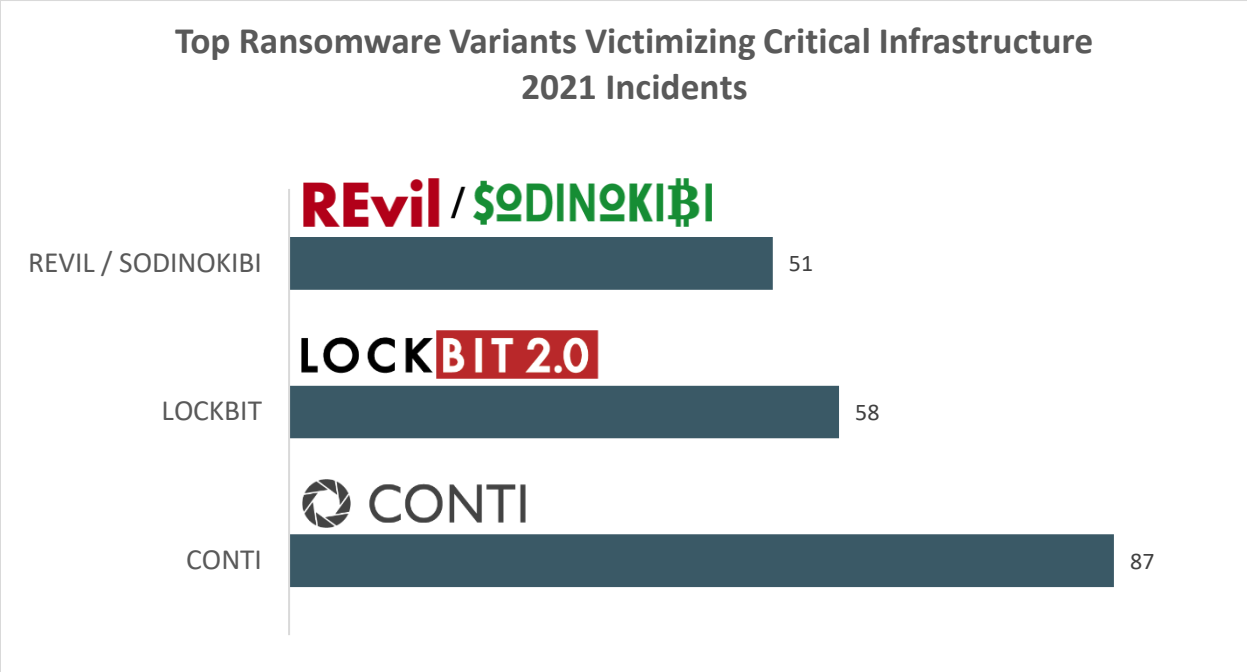
In October 2021, the IC3 posted a Joint Cybersecurity Advisory (CSA) to ic3.gov regarding ongoing cyber threats to U.S. Water and Wastewater Systems. In September 2021, the IC3 posted a Private Industry Notification (PIN) which warned that ransomware attacks targeting the Food and Agriculture sector disrupt operations, cause financial loss, and negatively impact the food supply chain. In May 2021, the IC3 posted an FBI Liaison Alert System (FLASH) report that advised the FBI identified at least 16 CONTI ransomware attacks targeting US Healthcare and First Responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year. And in March 2021, the IC3 posted a FLASH warning that FBI reporting indicated an increase in PYSA ransomware targeting education institutions in 12 US states and the United Kingdom.

The IC3 received 649 complaints that indicated organizations belonging to a critical infrastructure sector were victims of a ransomware attack. Of the 16 critical infrastructure sectors, IC3 reporting indicated 14 sectors had at least 1 member that fell victim to a ransomware attack in 2021.[13]



[13] Accessibility description: Chart shows Infrastructure Sectors Victimized by Ransomware. Healthcare and Public Health was highest with 148 followed by Financial Services 89; Information Technology 74; Critical Manufacturing 65; Government Facilities 60; Commercial Facilities 56; Food and Agriculture 52; Transportation 38; Energy 31; Communications 17; Chemical 12; Water and Wastewater Systems 4; Emergency Services 2; Defense Industrial Base 1.

Of the known ransomware variants reported to IC3, the three top variants that victimized a member of a critical infrastructure sector were CONTI, LockBit, and REvil/Sodinokibi.



[14]

According to information submitted to the IC3, CONTI most frequently victimized the Critical Manufacturing, Commercial Facilities, and Food and Agriculture sectors. LockBit most frequently victimized the Government Facilities, Healthcare and Public Health, and Financial Services sectors. REvil/Sodinokibi most frequently victimized the Financial Services, Information Technology, and Healthcare and Public Health sectors.

Of all critical infrastructure sectors reportedly victimized by ransomware in 2021, the Healthcare and Public Health, Financial Services, and Information Technology sectors were the most frequent victims. The IC3 anticipates an increase in critical infrastructure victimization in 2022.

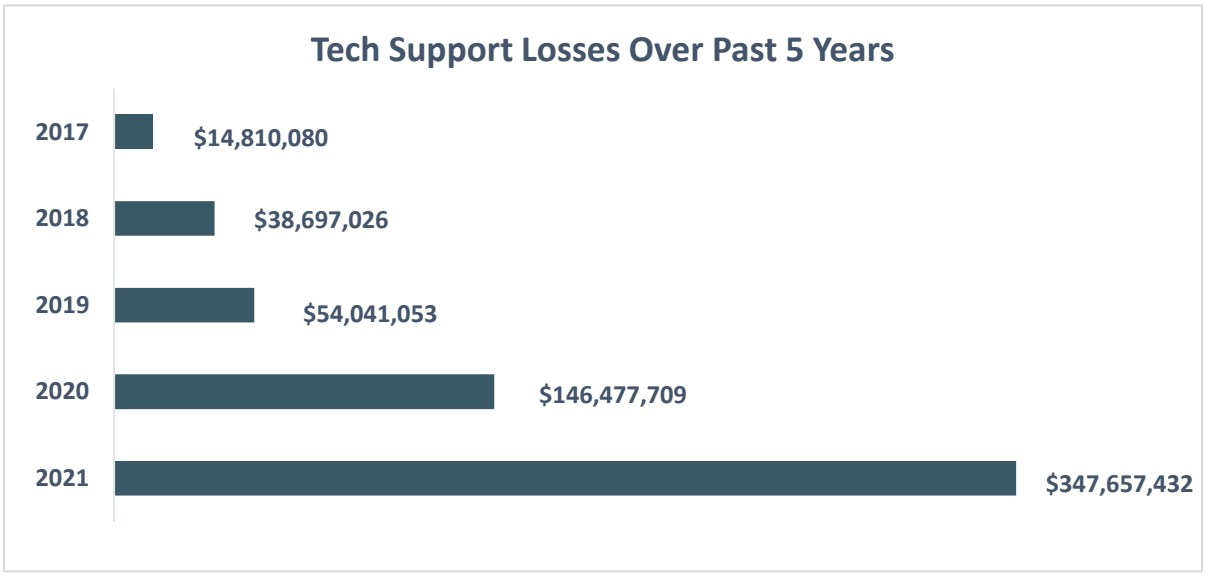
The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and /or fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local FBI field office or the IC3. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

[14] Accessibility description: Chart shows top variants Victimizing Critical Infrastructure 2021 Incidents. REvil/Sodinokibi, Locbit, and CONTI.

TECH SUPPORT FRAUD[15]

Tech Support Fraud involves a criminal claiming to provide customer, security, or technical support or service to defraud unwitting individuals. Criminals may pose as support or service representatives offering to resolve such issues as a compromised email or bank account, a virus on a computer, or a software license renewal.

Many victims report being directed to make wire transfers to overseas accounts or purchase large amounts of prepaid cards. In 2021, the IC3 received 23,903 complaints related to Tech Support Fraud from victims in 70 countries. The losses amounted to more than $347 million, which represents a 137 percent increase in losses from 2020. Most victims, almost 60 percent, report to be over 60 years of age, and experience at least 68 percent of the losses (almost $238 million).



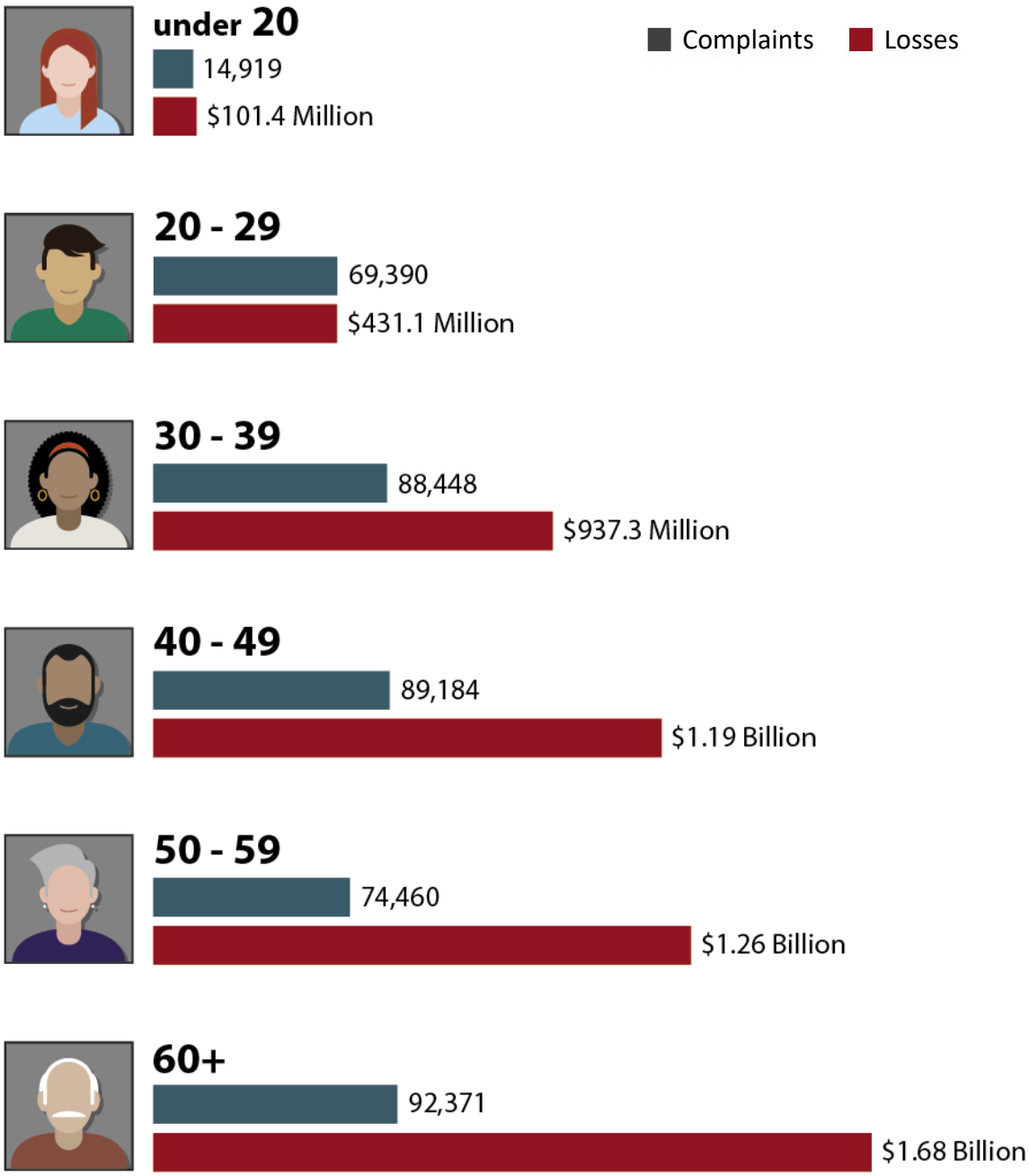
Tech support scammers continue to impersonate well-known tech companies, offering to fix non-existent technology issues or renew fraudulent software or security subscriptions. However, in 2021, the IC3 observed an increase in complaints reporting the impersonation of customer support, which has taken on a variety of forms, such as financial and banking institutions, utility companies, or virtual currency exchanges.

[15] Accessibility description: Chart shows Tech Support Losses Over Past 5 Years.
2021 $347,657,432; 2020 $146,477,709; 2019 $54,041,053; 2018 $38,697,026; 2017 $14,810,080.

IC3 by the Numbers[16]

[16] Accessibility description: Image depicts key statistics regarding complaints and victim loss. Total losses of $6.9 billion were reported in 2021. The total number of complaints received since the year 2000 is over 6.5 million. IC3 has received approximately 552,000 complaints per year on average over the last five years, or more than 2,300 complaints per day.

2021 Victims by Age Group[17]

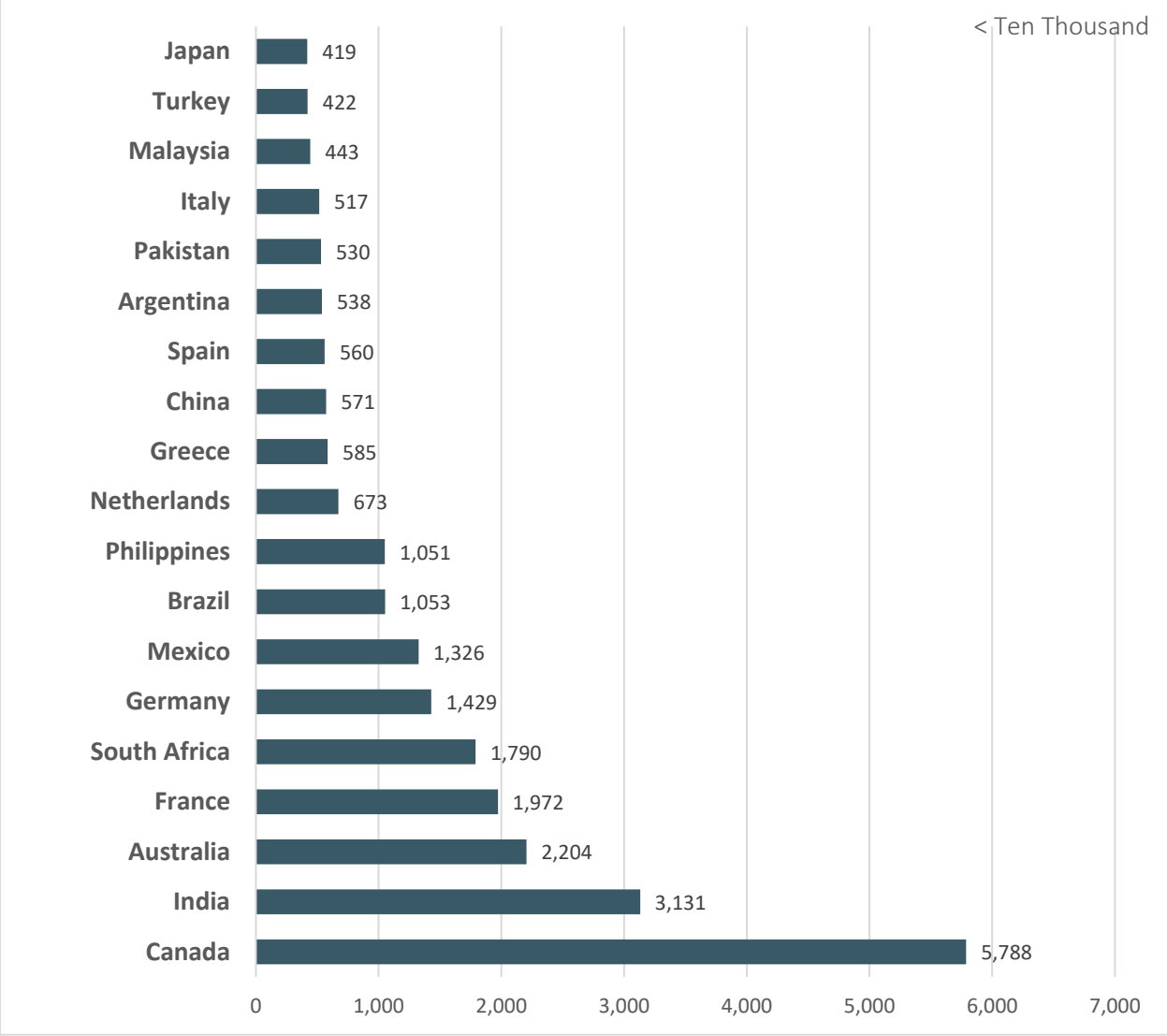


[17] Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix B for more information regarding IC3 data.

Accessibility description: Chart shows number of complaints and Loss for Victims by Age Group. Under 20 14,919 victims $101.4 Million losses; 20-29 69,390 Victims $431.1. Million losses; 30-39 88,448 Victims $937.3 Million losses; 40-49 89,184 victims $1.19 Billion losses; 50-59 74,460 Victims $1.26 Billion losses; 60+ 92,371 Victims $1.68 Billion losses.

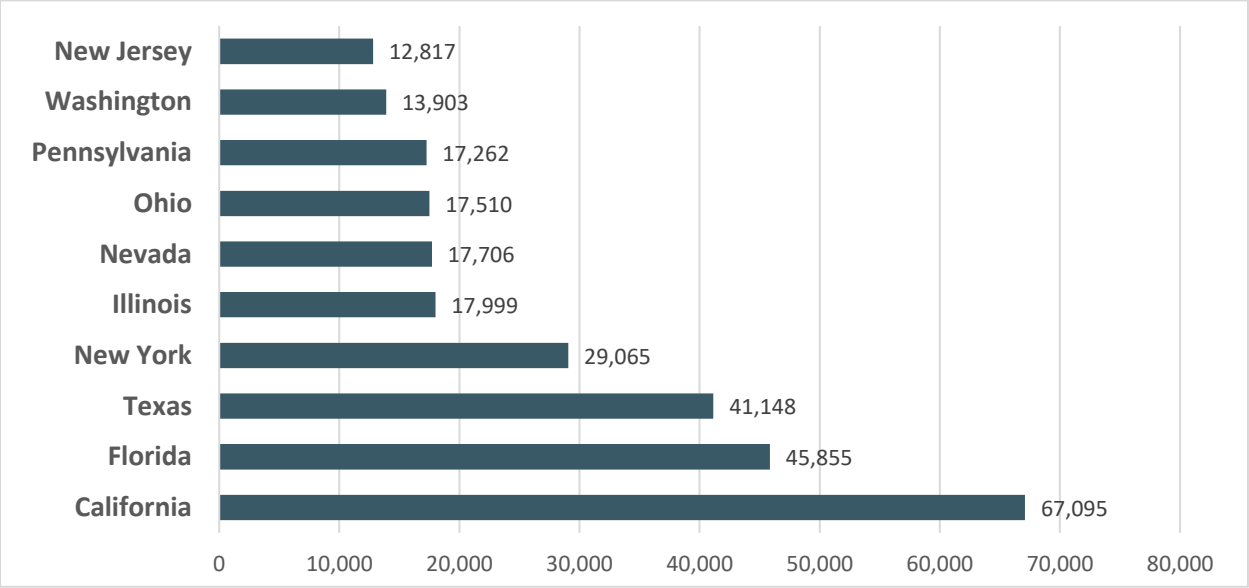
2021 - Top 20 International Victim Countries[18]

Compared to the United States

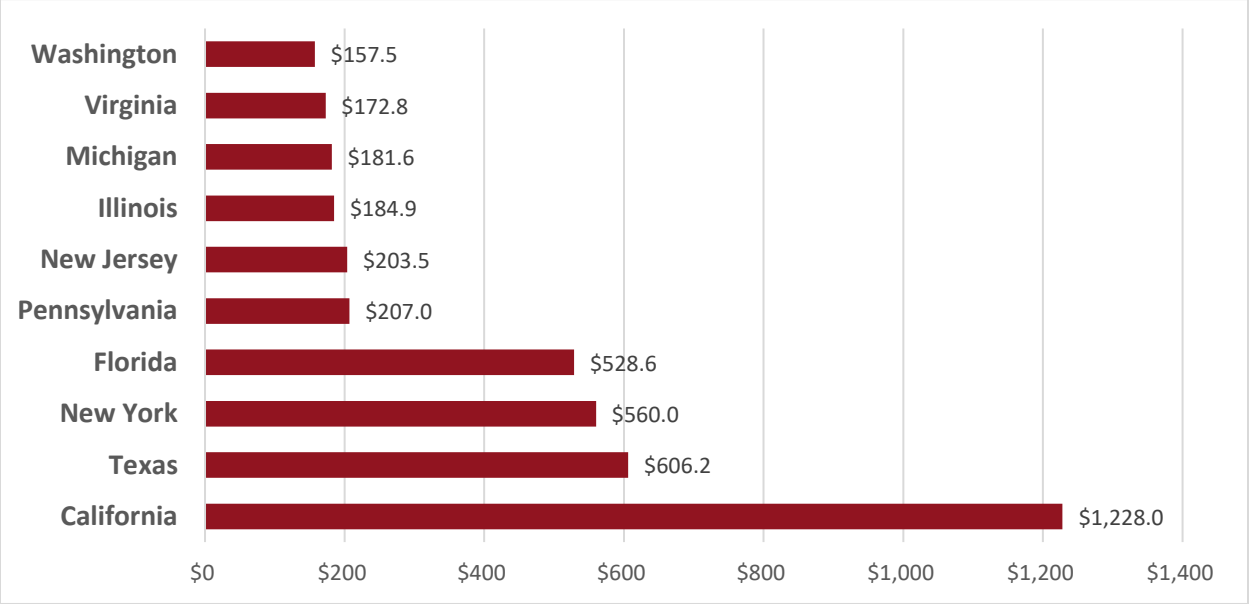


[18] Accessibility description: The charts list the top 20 countries by number of total victims as compared to the United States. The specific number of victims for each country are listed in ascending order to the right of the graph. Please see Appendix B for more information regarding IC3 data.

2021 - Top 10 States by Number of Victims[19]



2021 - Top 10 States by Victim Loss in $ Millions[20]



[19] Accessibility description: Chart depicts the top 10 states based on number of reporting victims are labeled. These include California, Florida, Texas, New York, Illinois, Nevada, Ohio, Pennsylvania, Washington, and New Jersey. Please see Appendix B for more information regarding IC3 data.

[20] Accessibility description: Chart depicts the top 10 states based on reported victim loss are labeled. These include California, Texas, New York, Florida, Pennsylvania, New Jersey, Illinois, Michigan, Virginia, and Washington. Please see Appendix B for more information regarding IC3 data.

2021 CRIME TYPES

By Victim Count			
Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing/Vishing/Smishing/Pharming	323,972	Government Impersonation	11,335
Non-Payment/Non-Delivery	82,478	Advanced Fee	11,034
Personal Data Breach	51,829	Overpayment	6,108
Identity Theft	51,629	Lottery/Sweepstakes/Inheritance	5,991
Extortion	39,360	IPR/Copyright and Counterfeit	4,270
Confidence Fraud/Romance	24,299	Ransomware	3,729
Tech Support	23,903	Crimes Against Children	2,167
Investment	20,561	Corporate Data Breach	1,287
BEC/EAC	19,954	Civil Matter	1,118
Spoofing	18,522	Denial of Service/TDoS	1,104
Credit Card Fraud	16,750	Computer Intrusion	979
Employment	15,253	Malware/Scareware/Virus	810
Other	12,346	Health Care Related	578
Terrorism/Threats of Violence	12,346	Re-shipping	516
Real Estate/Rental	11,578	Gambling	395
*Descriptors**			
Social Media	36,034	Virtual Currency	34,202

*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

2021 Crime Types continued

By Victim Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
BEC/EAC	$2,395,953,296	Lottery/Sweepstakes/Inheritance	$71,289,089
Investment	$1,455,943,193	Extortion	$60,577,741
Confidence Fraud/Romance	$956,039,740	Ransomware	*$49,207,908
Personal Data Breach	$517,021,289	Employment	$47,231,023
Real Estate/Rental	$350,328,166	Phishing/Vishing/Smishing/Pharming	$44,213,707
Tech Support	$347,657,432	Overpayment	$33,407,671
Non-Payment/Non-Delivery	$337,493,071	Computer Intrusion	$19,603,037
Identity Theft	$278,267,918	IPR/Copyright/Counterfeit	$16,365,011
Credit Card Fraud	$172,998,385	Health Care Related	$7,042,942
Corporate Data Breach	$151,568,225	Malware/Scareware/Virus	$5,596,889
Government Impersonation	$142,643,253	Terrorism/Threats of Violence	$4,390,720
Advanced Fee	$98,694,137	Gambling	$1,940,237
Civil Matter	$85,049,939	Re-shipping	$631,466
Spoofing	$82,169,806	Denial of Service/TDos	$217,981
Other	$75,837,524	Crimes Against Children	$198,950

*Descriptors***			
Social Media	$235,279,057	Virtual Currency	$1,602,647,341

* Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.

**These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

Last 3 Year Complaint Count Comparison

By Victim Count			▼ ▲ = Trend from previous Year		
Crime Type	***2021***		*2020*		*2019*
Advanced Fee	**11,034**	▼	13,020	▼	14,607	▼
BEC/EAC	**19,954**	▲	19,369	▼	23,775	▲
Civil Matter	**1,118**	▲	968	▲	908	▲
Confidence Fraud/Romance	**24,299**	▲	23,751	▲	19,473	▲
Corporate Data Breach	**1,287**	▼	2,794	▲	1,795	▼
Credit Card Fraud	**16,750**	▼	17,614	▲	14,378	▼
Crimes Against Children	**2,167**	▼	3,202	▲	1,312	▼
Denial of Service/TDoS	**1,104**	▼	2,018	▲	1,353	▼
Employment	**15,253**	▼	16,879	▲	14,493	▼
Extortion	**39,360**	▼	76,741	▲	43,101	▼
Gambling	**395**	▲	391	▲	262	▲
Government Impersonation	**11,335**	▼	12,827	▼	13,873	▲
Health Care Related	**578**	▼	1,383	▲	657	▲
Identity Theft	**51,629**	▲	43,330	▲	16,053	▼
Investment	**20,561**	▲	8,788	▲	3,999	▲
IPR/Copyright and Counterfeit	**4,270**	▲	4,213	▲	3,892	▲
Lottery/Sweepstakes/Inheritance	**5,991**	▼	8,501	▲	7,767	▲
Malware/Scareware/Virus	**810**	▼	1,423	▼	2,373	▼
Non-Payment/Non-Delivery	**82,478**	▼	108,869	▲	61,832	▼
Other	**12,346**	▲	10,372	▼	10,842	▲
Overpayment	**6,108**	▼	10,988	▼	15,395	▼
Personal Data Breach	**51,829**	▲	45,330	▲	38,218	▼
Phishing/Vishing/Smishing/Pharming	**323,972**	▲	241,342	▲	114,702	▲
Ransomware	**3,729**	▲	2,474	▲	2,047	▲
Real Estate/Rental	**11,578**	▼	13,638	▲	11,677	▲
Re-Shipping	**516**	▼	883	▼	929	▲
Spoofing	**18,522**	▼	28,218	▲	25,789	▲
Tech Support	**23,903**	▲	15,421	▲	13,633	▼
Terrorism/Threats of Violence	**12,346**	▼	20,669	▲	15,563	▼

Last 3 Year Complaint Loss Comparison

By Victim Loss			▼ ▲ = Trend from previous Year		
Crime Type	***2021***		*2020*		*2019*
Advanced Fee	**$98,694,137**	▲	$83,215,405	▼	$100,602,297	▲
BEC/EAC	**$2,395,953,296**	▲	$1,866,642,107	▲	$1,776,549,688	▲
Civil Matter	**$85,049,939**	▲	$24,915,958	▲	$20,242,867	▲
Confidence Fraud/Romance	**$956,039,739**	▲	$600,249,821	▲	$475,014,032	▲
Corporate Data Breach	**$151,568,225**	▲	$128,916,648	▲	$53,398,278	▼
Credit Card Fraud	**$172,998,385**	▲	$129,820,792	▲	$111,491,163	▲
Crimes Against Children	**$198,950**	▼	$660,044	▼	$975,311	▲
Denial of Service/TDoS	**$217,981**	▼	$512,127	▼	$7,598,198	▲
Employment	**$47,231,023**	▼	$62,314,015	▲	$42,618,705	▼
Extortion	**$60,577,741**	▼	$70,935,939	▼	$107,498,956	▲
Gambling	**$1,940,237**	▼	$3,961,508	▲	$1,458,118	▲
Government Impersonation	**$142,643.253**	▲	$109,938,030	▼	$124,292,606	▲
Health Care Related	**$7,042,942**	▼	$29,042,515	▲	$1,128,838	▼
Identity Theft	**$278,267,918**	▲	$219,484,699	▲	$160,305,789	▲
Investment	**$1,455,943,193**	▲	$336,469,000	▲	$222,186,195	▼
IPR/Copyright and Counterfeit	**$16,365,011**	▲	$5,910,617	▼	$10,293,307	▼
Lottery/Sweepstakes/Inheritance	**$71,289,089**	▲	$61,111,319	▲	$48,642,332	▼
Malware/Scareware/Virus	**$5,596,889**	▼	$6,904,054	▲	$2,009,119	▼
Non-Payment/Non-Delivery	**$337,493,071**	▲	$265,011,249	▲	$196,563,497	▲
Other	**$75,837,524**	▼	$101,523,082	▲	$66,223,160	▲
Overpayment	**$33,407,671**	▼	$51,039,922	▼	$55,820,212	▲
Personal Data Breach	**$517,021,289**	▲	$194,473,055	▲	$120,102,501	▼
Phishing/Vishing/Smishing/Pharming	**$44,213,707**	▼	$54,241,075	▼	$57,836,379	▲
Ransomware	**$49,207,908**	▲	$29,157,405	▲	$8,965,847	▲
Real Estate/Rental	**$350,328,166**	▲	$213,196,082	▼	$221,365,911	▲
Re-Shipping	**$631,466**	▼	$3,095,265	▲	$1,772,692	▲
Spoofing	**$82,169,806**	▼	$216,513,728	▼	$300,478,433	▲
Tech Support	**$347,657,432**	▲	$146,477,709	▲	$54,041,053	▲
Terrorism/Threats of Violence	**$4,390,720**	▼	$6,547,449	▼	$19,916,243	▲

Overall State Statistics

Victim per State*					
Rank	*State*	*Victims*	*Rank*	*State*	*Victims*
1	California	67,095	30	Louisiana	4,248
2	Florida	45,855	31	Utah	4,242
3	Texas	41,148	32	Oklahoma	4,156
4	New York	29,065	33	Arkansas	2,745
5	Illinois	17,999	34	Kansas	2,693
6	Nevada	17,706	35	New Mexico	2,644
7	Ohio	17,510	36	Nebraska	2,407
8	Pennsylvania	17,262	37	Mississippi	2,170
9	Washington	13,903	38	West Virginia	2,135
10	New Jersey	12,817	39	Delaware	2,132
11	Arizona	12,375	40	District of Columbia	2,103
12	Virginia	11,785	41	Puerto Rico	1,923
13	Georgia	11,776	42	Idaho	1,882
14	Maryland	11,693	43	Alaska	1,787
15	Indiana	11,399	44	Hawaii	1,615
16	Michigan	10,930	45	New Hampshire	1,487
17	Colorado	10,537	46	Maine	1,402
18	North Carolina	10,363	47	Rhode Island	1,205
19	Missouri	9,692	48	Montana	1,188
20	Massachusetts	9,174	49	South Dakota	951
21	Iowa	8,853	50	Wyoming	735
22	Wisconsin	8,646	51	Vermont	715
23	Kentucky	7,148	52	North Dakota	670
24	Tennessee	7,129	53	Virgin Islands, U.S.	100
25	Oregon	5,954	54	U.S. Minor Outlying Islands	93
26	Minnesota	5,844	55	Guam	64
27	South Carolina	5,426	56	Northern Mariana Islands	29
28	Alabama	5,347	57	American Samoa	25
29	Connecticut	4,524			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

Overall State Statistics continued

Total Victim Losses by State*

Rank	State	Loss	Rank	State	Loss
1	California	$1,227,989,139	30	Louisiana	$38,783,908
2	Texas	$606,179,646	31	Kentucky	$37,953,949
3	New York	$559,965,598	32	Iowa	$33,821,569
4	Florida	$528,573,929	33	Kansas	$26,031,546
5	Pennsylvania	$206,982,032	34	North Dakota	$21,246,355
6	New Jersey	$203,510,341	35	Mississippi	$20,578,948
7	Illinois	$184,860,704	36	District of Columbia	$20,096,921
8	Michigan	$181,622,993	37	Nebraska	$19,743,241
9	Virginia	$172,767,012	38	Hawaii	$18,964,018
10	Washington	$157,454,331	39	South Dakota	$18,131,095
11	Massachusetts	$150,384,982	40	Idaho	$17,682,386
12	Georgia	$143,998,767	41	Arkansas	$15,302,829
13	Ohio	$133,666,156	42	New Hampshire	$15,302,618
14	Colorado	$130,631,286	43	Delaware	$15,041,717
15	Arizona	$124,158,717	44	Puerto Rico	$14,650,062
16	Tennessee	$103,960,100	45	Alaska	$13,070,648
17	Maryland	$99,110,757	46	New Mexico	$12,761,850
18	North Carolina	$91,416,226	47	Rhode Island	$11,191,079
19	Nevada	$83,712,410	48	Wyoming	$10,249,609
20	Minnesota	$82,535,103	49	Montana	$10,107,283
21	Oregon	$75,739,646	50	Vermont	$9,826,787
22	Connecticut	$72,476,672	51	West Virginia	$9,453,607
23	Utah	$65,131,003	52	Maine	$7,261,234
24	Indiana	$60,524,818	53	Guam	$2,168,956
25	Missouri	$53,797,188	54	Virgin Islands, U.S.	$895,946
26	Wisconsin	$51,816,862	55	Northern Mariana Islands	$705,244
27	Oklahoma	$50,196,339	56	U.S. Minor Outlying Islands	$403,844
28	Alabama	$49,522,904	57	American Samoa	$177,533
29	South Carolina	$42,768,322			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

Overall State Statistics continued

Count by Subject per State*					
Rank	*State*	*Subjects*	*Rank*	*State*	*Subjects*
1	California	27,706	30	Nebraska	1,243
2	Texas	13,518	31	Kentucky	1,238
3	Florida	11,527	32	District of Columbia	1,107
4	New York	10,696	33	Utah	1,063
5	Maryland	5,244	34	Delaware	924
6	Ohio	5,182	35	New Mexico	893
7	Pennsylvania	5,168	36	Kansas	876
8	Illinois	4,587	37	West Virginia	863
9	Georgia	4,521	38	Arkansas	831
10	New Jersey	3,913	39	Iowa	723
11	Washington	3,586	40	Mississippi	714
12	Virginia	3,542	41	Montana	681
13	Arizona	3,485	42	Maine	507
14	North Carolina	3,316	43	Idaho	486
15	Nevada	3,308	44	New Hampshire	467
16	Colorado	2,885	45	Hawaii	435
17	Michigan	2,605	46	Alaska	429
18	Tennessee	2,384	47	Puerto Rico	346
19	Massachusetts	2,018	48	Rhode Island	318
20	Indiana	1,976	49	North Dakota	297
21	Oklahoma	1,929	50	Wyoming	251
22	Missouri	1,646	51	South Dakota	216
23	Oregon	1,598	52	Vermont	189
24	Minnesota	1,553	53	U.S. Minor Outlying Islands	34
25	Alabama	1,520	54	Virgin Islands, U.S.	14
26	Connecticut	1,499	55	Guam	11
27	Louisiana	1,398	56	Northern Mariana Islands	7
28	South Carolina	1,358	57	American Samoa	3
29	Wisconsin	1,316			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

Overall State Statistics continued

Subject Earnings per Destination State*

Rank	State	Loss	Rank	State	Loss
1	California	$404,965,496	30	South Carolina	$10,406,812
2	New York	$320,011,292	31	Iowa	$7,960,272
3	Florida	$174,884,203	32	Wyoming	$7,007,308
4	Texas	$168,153,129	33	Idaho	$6,879,088
5	Colorado	$96,949,691	34	Connecticut	$6,586,016
6	Illinois	$82,985,601	35	Kansas	$6,527,306
7	Ohio	$65,567,505	36	New Mexico	$6,441,444
8	Georgia	$62,682,196	37	Kentucky	$6,260,280
9	Washington	$49,643,646	38	Arkansas	$5,511,079
10	New Jersey	$46,773,594	39	Delaware	$5,404,683
11	Nevada	$46,441,562	40	Hawaii	$5,312,553
12	Pennsylvania	$44,661,540	41	Nebraska	$5,156,069
13	Arizona	$44,490,075	42	New Hampshire	$5,082,033
14	Louisiana	$43,427,842	43	Mississippi	$4,245,861
15	North Carolina	$43,281,815	44	Puerto Rico	$4,067,734
16	Virginia	$42,989,608	45	Maine	$3,445,411
17	Maryland	$33,912,104	46	Vermont	$3,357,692
18	Massachusetts	$29,327,619	47	Rhode Island	$3,307,726
19	Michigan	$28,857,054	48	North Dakota	$3,174,006
20	Oklahoma	$19,278,395	49	Montana	$2,946,504
21	Minnesota	$19,039,734	50	Alaska	$2,773,302
22	Tennessee	$18,580,987	51	South Dakota	$2,413,398
23	Utah	$17,137,321	52	West Virginia	$2,269,994
24	Missouri	$16,619,864	53	Northern Mariana Islands	$107,000
25	District of Columbia	$15,656,649	54	U.S. Minor Outlying Islands	$77,350
26	Wisconsin	$14,886,212	55	Virgin Islands, U.S.	$44,453
27	Alabama	$14,639,799	56	Guam	$3,932
28	Indiana	$14,634,699	57	American Samoa	$420
29	Oregon	$10,561,887			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.

Appendix A: Definitions

Advanced Fee: An individual pays money to someone in anticipation of receiving something of greater value in return, but instead, receives significantly less than expected or nothing.

Business Email Compromise/Email Account Compromise: BEC is a scam targeting businesses (not individuals) working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam which targets individuals. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Civil Matter: Civil litigation generally includes all disputes formally submitted to a court, about any subject in which one party is claimed to have committed a wrong but not a crime. In general, this is the legal process most people think of when the word "lawsuit" is used.

Computer Intrusion: Unauthorized access or exceeding authorized access into a protected computer system. A protected computer system is one owned or used by the US Government, a financial institution, or any business. This typically excludes personally owned systems and devices.

Confidence/Romance Fraud: An individual believes they are in a relationship (family, friendly, or romantic) and are tricked into sending money, personal and financial information, or items of value to the perpetrator or to launder money or items to assist the perpetrator. This includes the Grandparent's Scheme and any scheme in which the perpetrator preys on the complainant's "heartstrings".

Corporate Data Breach: A data breach within a corporation or business where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.

Credit Card Fraud: Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism (ACH. EFT, recurring charge, etc.) as a fraudulent source of funds in a transaction.

Crimes Against Children: Anything related to the exploitation of children, including child abuse.

Denial of Service/TDoS: A Denial of Service (DoS) attack floods a network/system, or a Telephony Denial of Service (TDoS) floods a voice service with multiple requests, slowing down or interrupting service.

Employment: An individual believes they are legitimately employed and loses money, or launders money/items during the course of their employment.

Extortion: Unlawful extraction of money or property through intimidation or undue exercise of authority. It may include threats of physical harm, criminal prosecution, or public exposure.

Gambling: Online gambling, also known as Internet gambling and iGambling, is a general term for gambling using the Internet.

Government Impersonation: A government official is impersonated in an attempt to collect money.

Health Care Related: A scheme attempting to defraud private or government health care programs which usually involving health care providers, companies, or individuals. Schemes may include offers for fake insurance cards, health insurance marketplace assistance, stolen health information, or various other scams and/or any scheme involving medications, supplements, weight loss products, or diversion/pill mill practices. These scams are often initiated through spam email, Internet advertisements, links in forums/social media, and fraudulent websites.

IPR/Copyright and Counterfeit: The illegal theft and use of others' ideas, inventions, and creative expressions – what's called intellectual property – everything from trade secrets and proprietary products and parts to movies, music, and software.

Identity Theft: Someone steals and uses personal identifying information, like a name or Social Security number, without permission to commit fraud or other crimes and/or (Account Takeover) a fraudster obtains account information to perpetrate fraud on existing accounts.

Investment: Deceptive practice that induces investors to make purchases based on false information. These scams usually offer the victims large returns with minimal risk. (Retirement, 401K, Ponzi, Pyramid, etc.).

Lottery/Sweepstakes/Inheritance: An Individual is contacted about winning a lottery or sweepstakes they never entered, or to collect on an inheritance from an unknown relative.

Malware/Scareware/Virus: Software or code intended to damage, disable, or capable of copying itself onto a computer and/or computer systems to have a detrimental effect or destroy data.

Non-Payment/Non-Delivery: Goods or services are shipped, and payment is never rendered (non-payment). Payment is sent, and goods or services are never received, or are of lesser quality (non-delivery).

Overpayment: An individual is sent a payment/commission and is instructed to keep a portion of the payment and send the remainder to another individual or business.

Personal Data Breach: A leak/spill of personal data which is released from a secure location to an untrusted environment. Also, a security incident in which an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.

Phishing/Vishing/Smishing/Pharming: The use of unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

Ransomware: A type of malicious software designed to block access to a computer system until money is paid.

Re-shipping: Individuals receive packages at their residence and subsequently repackage the merchandise for shipment, usually abroad.

Real Estate/Rental: Loss of funds from a real estate investment or fraud involving rental or timeshare property.

Spoofing: Contact information (phone number, email, and website) is deliberately falsified to mislead and appear to be from a legitimate source. For example, spoofed phone numbers making mass robo-calls; spoofed emails sending mass spam; forged websites used to mislead and gather personal information. Often used in connection with other crime types.

Social Media: A complaint alleging the use of social networking or social media (Facebook, Twitter, Instagram, chat rooms, etc.) as a vector for fraud. Social Media does not include dating sites.

Tech Support: Subject posing as technical or customer support/service.

Terrorism/Threats of Violence: Terrorism is violent acts intended to create fear that are perpetrated for a religious, political, or ideological goal and deliberately target or disregard the safety of non-combatants. Threats of Violence refers to an expression of an intention to inflict pain, injury, or punishment, which does not refer to the requirement of payment.

Virtual Currency: A complaint mentioning a form of virtual cryptocurrency, such as Bitcoin, Litecoin, or Potcoin.

Appendix B: Additional Information about IC3 Data

- Each complaint is reviewed by an IC3 analyst. The analyst categorizes the complaint according to the crime type(s) that are appropriate. Additionally, the analyst will adjust the loss amount if the complaint data does not support the loss amount reported.
- One complaint may have multiple crime types.
- Some complainants may have filed more than once, creating a possible duplicate complaint.
- All location-based reports are generated from information entered when known/provided by the complainant.
- Losses reported in foreign currencies are converted to U.S. dollars when possible.
- Complaint counts represent the number of individual complaints received from each state and do not represent the number of individuals filing a complaint.
- Victim is identified as the individual filing a complaint.
- Subject is identified as the individual perpetrating the scam as reported by the victim.
- "Count by Subject per state" is the number of subjects per state, as reported by victims.
- "Subject earnings per Destination State" is the amount swindled by the subject, as reported by the victim, per state.

Core Cybersecurity Threats and Effective Controls for Small Firms

Sound cybersecurity practices are a key focus of member firms and FINRA, especially given the evolving nature, increasing frequency and mounting sophistication of cybersecurity attacks —as well as the potential for harm to investors, member firms and the markets. Cybersecurity is one of the principal operational risks facing broker-dealers, and FINRA expects member firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations.

The following list updates and expands on the Core Cybersecurity Controls for Small Firms provided in the Report on Selected Cybersecurity Practices – 2018 (2018 Report) by identifying key cybersecurity risks currently faced by small firms and helping them enhance their customer information protection, and cybersecurity written supervisory programs (WSPs) and related controls, including:

- Highlighting the most common and recent categories of cybersecurity threats faced by small firms, including questions to assist firms with addressing such threats;
- Providing a summary of effective core controls small firms should consider, as well as relevant questions for consideration to evaluate their current cybersecurity programs; and
- Including appendices with a glossary of relevant terms and additional resources.

Regulatory Obligations

Rule 30 of the U.S. Securities and Exchange Commission's (SEC) 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. Cybersecurity remains one of the principal operational risks facing broker-dealers and FINRA 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 their 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.

Contact Us

Questions related to this tool or other Cybersecurity topics can be sent to Member Supervision's CyberTech team at cybertech@finra.org.

COMMON CYBERSECURITY THREATS FOR SMALL FIRMS

1 IMPOSTER WEBSITES

☐ Reviewed ✔

Small firms frequently report to FINRA cybersecurity risks related to imposter websites,[1] where fraudsters use registered representatives' names, firm information or both to establish websites that market investment services and products. These sites attempt to steal both personal information and investor funds by leading site visitors to believe that they are investing in a legitimate business or legitimate products. Firms may want to consider asking the following questions, where applicable, with respect to how they monitor for, and address, imposter websites:

- How does your firm monitor for imposter websites that may be impersonating your firm or your registered representatives?
  - Has your firm registered website name variations, including common misspellings or visually similar character substitutions?
  - Does your firm use social media or website monitoring services to watch for imposter websites?
- How does your firm address imposter websites once they are identified? If your firm becomes aware of an imposter website, has it addressed the concern with the hosting provider and domain name registrar, sought assistance from specialists and informed regulators and customers?[2]

2 PHISHING

☐ Reviewed ✔

Phishing is one of the most common cybersecurity threats affecting firms[3] – it may take a variety of forms, but all phishing attempts try to convince the recipient to provide information or take action. The fraudsters typically try to disguise themselves as a trustworthy entity or individual via email, instant message, phone call or other communication, where they request personally identifiable information (PII) (such as Social Security numbers, usernames or passwords), direct the recipient to click on a malicious link, open an infected attachment or application, or attempt to initiate a fraudulent wire transfer or transaction. Firms may want to consider asking the following questions, where applicable, with respect to how they identify, prevent and mitigate phishing attempts:

- Do your firm's policies and procedures address phishing by, for example:
  - identifying phishing emails;

---

[1] *See* FINRA *Information Notice - 4/29/19* (Imposter Websites Impacting Member Firms) and *Regulatory Notice 20-30* (Fraudsters Using Registered Representatives Names to Establish Imposter Websites).

[2] *See Information Notice - 4/29/19* (Imposter Websites Impacting Member Firms).

[3] See, *e.g.*, *Regulatory Notice 12-05* (Verification of Emailed Instructions to Transmit or Withdraw Assets From Customer Accounts); *Regulatory Notice 21-30* (FINRA Alerts Firms to a Phishing Email Campaign Using Multiple Imposter FINRA Domain Names); *Regulatory Notice 21-22* (FINRA Alerts Firms to Phishing Email From "FINRA Support" From the Domain Name "westour.org"); *Regulatory Notice 21-20* (FINRA Alerts Firms to Phishing Email Using "gateway-finra.org" Domain Name); *Regulatory Notice 20-27* (FINRA Alerts Firms to Use of Fake FINRA Domain Name); *Regulatory Notice 21-08* (FINRA Alerts Firms to Phishing Email Using "finra-online.com" Domain Name); and *Regulatory Notice 20-12* (FINRA Warns of Fraudulent Phishing Emails Purporting to be from FINRA).

- clarifying that staff should not click on any links or open any attachments in phishing emails;
- requiring deletion of phishing emails;
- developing a process to securely notify Information Technology (IT) administrators or compliance staff of phishing attempts;
- confirming requests for wire transfers of a certain type, or above a certain threshold, with the customer via telephone or in person; and
- ensuring proper resolution and remediation after phishing attacks?

- Has your firm implemented email scanning and filtering to monitor and block phishing and spam communication?
- Does your firm regularly conduct phishing email campaign simulations to evaluate employee understanding and compliance of its phishing policies and procedures?

3 CUSTOMER AND FIRM EMPLOYEE ACCOUNT TAKEOVERS (ATOs)

☐ Reviewed ✔

Customer and firm employee email ATOs have become an increasingly problematic area for firms. ATOs can occur either at customer or firm personnel accounts and usually begin with their email account being compromised. Fraudsters can gain unauthorized access to customer and firm employee email accounts through data breaches, phishing emails or websites that trick users into clicking on malicious links allowing them to execute unauthorized transactions in financial accounts, firm systems, bank accounts and credit cards. Fraudsters can also monitor those email accounts, view or download the information contained within messages and even add new email rules to hide legitimate correspondence. In addition, some fraudsters use synthetic identities to establish accounts to divert specific types of payments, such as congressional stimulus funds or unemployment payments, or to engage in automated clearing house (ACH) or wire fraud. Firms may want to consider asking the following questions, where applicable, with respect to how they identify, prevent and mitigate ATOs impacting broker-dealers or affiliates, as well as those impacting customer accounts:

For ATOs impacting broker-dealers or affiliates:

- Does your firm require multi-factor authentication (MFA) for external access to email systems, vendor portals or other systems that may contain confidential information?
- Does your firm have automated monitoring, alerting or both for suspicious logins?
- For high-risk transactions (*e.g.*, third-party money movements) does your firm have a process to validate these requests?

For ATOs impacting customer accounts:

- What documentary identification (*e.g.*, drivers' licenses, passports) and non-documentary methods (*e.g.*, contacting the customer, obtaining a customer's financial statement) does your firm use to verify customers' identities when establishing online accounts?
- What approaches does your firm take to verify customer identities when they access their online accounts (*e.g.*, MFA, adaptive authentication) and initiate transfer requests (*e.g.*, reviewing the Internet Protocol (IP) address of requests made online or through a mobile device for consistency with past legitimate transactions)?
- How does your firm proactively address potential or reported customer ATOs? What practices has your firm implemented to restore customer account access in a secure and timely manner?
- Do your firm's Suspicious Activity Reporting (SAR) procedures address ACH or wire fraud? Does your firm collaborate with its clearing firm to allocate responsibilities for handling ACH or wire transactions?

- Does your firm educate its customers on account security? Does your firm provide resources to its customers to help them identify potential security threats (*e.g.*, email or SMS text messages for certain types of account activity)?

4 MALWARE

☐ Reviewed ✔

Malware is a catch-all term for multiple types of malicious software (*e.g.*, viruses, spyware, worms) designed to cause damage to a stand-alone or networked computer. Malware most often originates from phishing emails where a user clicked on a link or opened an attachment. Once activated, it can mine a firm's system for PII and sensitive data; erase data; steal credentials; alter, corrupt or delete a firm's files and data; take over an email account; and even hijack device operations or computer-controlled hardware. Firms may want to consider asking the following questions, where applicable, with respect to how they identify, prevent and respond to malware attacks:

- How does your firm train employees to recognize and report cyberattacks involving malware?
- What preventative measures does your firm take (*e.g.*, endpoint malware protection) to defend against malware?
- How does your firm monitor for indications of malware on your firm's systems?
- How does your firm's incident response plan address malware infections?
- How does your firm incorporate threat intelligence regarding newly-identified instances of viruses or other types of malware into its IT infrastructure?

5 RANSOMWARE

☐ Reviewed ✔

Ransomware attacks are an increasingly common threat for small firms, and can quickly cripple their business operations, as well as expose firms to risks of data exfiltration and publication. This type of highly sophisticated malware commonly encrypts a firm's files, databases or applications to prevent firm employees from accessing them until a ransom demand is paid to the fraudster. Firms may want to consider asking the following questions, where applicable, with respect to how they identify, prevent and respond to ransomware attacks:

- Has the firm evaluated capabilities to detect and block sophisticated attacks, using tools such as endpoint detection and response (EDR), a host-based intrusion detection system (HIDS) and a host-based intrusion prevention system (HIPS)?
- Does your firm keep offline backups of systems and data? Are recovery capabilities tested on a regular basis?
- Does your firm's incident response plan include a scenario for potential ransomware attacks? If so, does your plan address factors such as:
    - making cybersecurity insurance claims;
    - engaging cybersecurity experts to conduct forensics investigations and to assist in recovery efforts;
    - assessing and mitigating the impact of these attacks; and
    - notifying affected parties (*e.g.*, customers, employees, regulators) as required by data breach notification laws applicable to your firm?

6 DATA BREACHES

☐ Reviewed ✔

Data breaches are another serious threat to small firms that can expose sensitive customer or firm information to an unauthorized party and may result in customer harm, reputational damage to a firm or both. If a data breach has been identified, firms must determine whether sensitive data is impacted and the various data privacy concerns, including the required notifications to regulators and customers because of the breach. Firms may want to consider asking the following questions, where applicable, with respect to how they investigate, monitor for, prevent and respond to data breaches:

- How does your firm investigate data breaches?
- Do your firm's contracts with vendors define "breach" – in the context of data and systems the vendor is involved with – as well as address the manner and timing of the vendor's notification to the data owner of a security breach, and the requirements as to who is responsible for notifying customers along with any related costs?
- Has your firm established a formal data loss prevention (DLP) program and applicable WSPs to monitor and prevent data breaches?
- Does your firm regularly train employees on effective practices for preventing data breaches (*e.g.*, appropriately handling customer requests for username and password changes; identifying social engineering activities from fraudsters)?
- Does your firm have a process to notify regulators and customers about data breaches?

EFFECTIVE CORE CYBERSECURITY CONTROLS FOR SMALL FIRMS

The following are some of the effective cybersecurity controls observed at small firms they should consider, as well as relevant questions for consideration they could use to evaluate their current cybersecurity programs. In addition to the following controls, FINRA has provided a number of cybersecurity resources for small firms that provide additional information on these and other controls, including the Cybersecurity and Technology Governance section of the 2022 Report on FINRA's Examination and Risk Monitoring Program, the 2015 FINRA Report on Cybersecurity Practices, the 2018 Report, the Small Firm Cybersecurity Checklist and the Cybersecurity Topic Page.

1 GOVERNANCE AND RISK MANAGEMENT

☐ Reviewed ✔

A firm's governance framework should enable it to become aware of relevant cybersecurity risks, estimate their severity and decide how to manage (*i.e.*, to accept, mitigate, transfer or avoid) each risk. Because there is no one-size-fits-all approach to cybersecurity, any governance framework should also include defined risk management policies, processes and structures coupled with relevant controls tailored to the nature of the cybersecurity risks the firm faces and the resources the firm has available. Firms may want to consider asking the following questions, where applicable, with respect to how they implement and maintain their cybersecurity-related governance framework and risk management policies:

- Does your firm use well-established, relevant industry frameworks[4] and standards to implement and maintain its cybersecurity program, including policies that are appropriate for the firm's size, business model and cybersecurity threat environment, particularly in areas such as:
    - data protection;
    - vendor management;
    - asset management;
    - risk management;
    - incident management and responses; and
    - branch controls?
- Has your firm conducted program risk assessments that include prioritization, tracking and follow up for all required implementation items for your cybersecurity program (*e.g.*, leveraging FINRA's Small Firm Cybersecurity Checklist)?
- Does your firm have a Chief Information Security Officer (CISO) or otherwise designate a single staff person to lead the firm's overall cybersecurity program, such as your firm's Chief Compliance Officer (CCO), IT leader or another member of senior management with sufficient knowledge of cybersecurity risks and controls?
- Has your firm established conducted documented meetings or assigned accountability for action items discussed in meetings?
- Does your firm's cybersecurity leadership engage your firm's executive management in all risk-based decisions aligned to the overall organization's goals and corresponding risks?

2 VENDOR MANAGEMENT

☐ Reviewed ✔

Member firms – including small firms – have increasingly leveraged vendors to implement systems and perform key functions (*e.g.*, customer relationship management systems, clearing arrangements, account statement generation) and often contract with Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs), respectively, to oversee their IT infrastructure and cybersecurity programs. Relying on vendors may help small firms reduce operating costs, improve efficiency and concentrate on core broker-dealer operations. However, 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.[5] Firms may want to consider asking the following questions, where applicable, with respect to how they select, conduct due diligence on and document relationships with cybersecurity vendors:

- Does your firm have a process for its decision-making on outsourcing, including the selection of cybersecurity vendors? Does this process engage key internal stakeholders and consider the impact of such outsourcing on its ability to comply with federal securities laws and regulations, and FINRA rules?

[4] Examples of these relevant frameworks include the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Center For Internet Security (CIS): Critical Security Controls and Federal Trade Commission (FTC): Cybersecurity for Small Business.

[5] Firms can find relevant guidance 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.

- Does your firm implement risk-based due diligence on vendors' cybersecurity practices critical to managing risks present in a firm's environment, including the ability to protect sensitive firm and customer non-public information?[6]
- Does your firm document relationships with vendors in written contracts that clearly define all parties' roles and responsibilities related to cybersecurity, such as evidencing compliance with federal and state securities laws and regulations, and FINRA rules; protection of sensitive firm and customer information; and notifications to your firm of cybersecurity events, and the vendor's efforts to remediate those events?
- Does your firm conduct independent, risk-based reviews to determine if vendors have experienced any cybersecurity events, data breaches or other security incidents? If so, does your firm evaluate the vendors' response to such events?

3 ACCESS CONTROLS

☐ Reviewed ✔

Small firms may face a unique set of challenges related to access controls due to their reliance on third party providers such as clearing firms, client management systems and IT services, including cloud-based providers. Third party providers may be especially appealing to small firms with fewer internal resources. However, this may result in vendor employees wearing multiple hats and having more access to systems and data than needed to fulfill their functions. Firms may want to consider asking the following questions, where applicable, with respect to how they grant access to firm and customer data, establish and enforce access and authentication controls, and detect and resolve anomalies within privileged accounts:

- Does your firm maintain WSPs in crucial areas, such as identity governance, onboarding, offboarding and periodic access reviews?
- Does your firm follow the Principle of Least Privilege when granting entitlements?
- Has your firm established identity and access management protocols for registered representatives and other staff, including managing the granting, maintenance and termination of access to firm and customer data?
- Does your firm enforce complex password standards and authentication controls (*e.g.*, MFA, password reuse, password change intervals, minimum length, character types and length, change frequency)?
- Has your firm implemented enhanced procedures (*e.g.*, monitoring, alerts) to detect anomalies in privileged accounts, such as a privileged user assigning herself or himself extra access rights, performing unauthorized work during off-hours or logging in from different geographic locations concurrently? Do your firm's procedures also account for logging the occurrence of anomalies, and how firms resolve them?
- Has your firm established physical access controls across office locations or access controls for remote work?

[6] *See id.*, at Section II for steps small firms can take when performing due diligence (*e.g.*, talking to industry peers; collecting and reviewing American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 reports, if available).

4 DATA PROTECTION

☐ Reviewed ✔

Data protection is one of the most important facets of a small firm's cybersecurity program. Small firms have information assets (*e.g.*, employee and customer information, firm sensitive data) that, if inadequately protected, could result in harm to the customers, individuals or the firm's reputation. DLP controls typically identify sensitive customer and firm data based on rules and then block or quarantine the transmission of the data whether by email, data upload or download, file transfer or other method; they can also prevent the inadvertent or malicious transmission of sensitive customer or firm information to unauthorized recipients. Firms may want to consider asking the following questions, where applicable, with respect to how they establish a formal DLP program, and applicable WSPs and controls, to protect sensitive customer and firm data:

- Has your firm identified where sensitive information is stored and transmitted?
- Has your firm established a formal DLP program and applicable WSPs to monitor and prevent data breaches?
- Does your firm regularly train employees on effective practices for preventing data breaches (*e.g.*, appropriately handling customer requests for username and password changes; identifying social engineering activities from fraudsters)?
- How does your firm implement encryption for confidential data at rest or in transit?
- Does your firm prohibit the storage of sensitive customer or firm data in unapproved or prohibited locations (*e.g.*, a file server, cloud provider or thumb drive transmitted without encryption)?
- What is your firm's policy regarding storing sensitive data on removable media or personal devices, as well its retention and secure disposal?
- How does the firm ensure that third parties involved in maintaining or storing sensitive information have reasonable data protection safeguards and cybersecurity controls? Are third parties' data protection responsibilities mutually agreed upon?

5 TECHNICAL CONTROLS

☐ Reviewed ✔

Technical controls perform many critical functions, such as keeping unauthorized individuals from gaining access to a system and detecting when a security violation has occurred. However, small firms may not have sufficient resources to ensure adequate safeguards around all possible attack surfaces, especially in today's hyperconnected world and ever-changing risk landscape. Small firms can use a cybersecurity risk assessment to determine which threats are most significant for each branch and then identify and implement appropriate technical and other controls to mitigate those threats. Firms may want to consider asking the following questions, where applicable, with respect to how they assess the cybersecurity risks at each of their branches, and implement appropriate controls to mitigate those risks:

- Does your firm understand where its cybersecurity risks lie, including its technology hardware and software asset inventories?
- Do your firm's staff in cybersecurity positions have the technical skillsets to properly configure tools and applications?
- How does your firm verify that its critical and sensitive systems have adequate protection and detection controls?

- What cyber hygiene controls (*e.g.*, endpoint, MFA, email encryption, DLP) does your firm implement?
- Does your firm enable automatic patching and updating features of operating systems and other software to help maintain the latest security controls?
- Does your firm prohibit the sharing of passwords among firm staff?

6 BRANCH CONTROLS

☐ Reviewed ✔

Overseeing IT and cybersecurity controls across a branch network can be especially challenging for small firms, including firms with independent contractor models. A branch network may present challenges for a firm' seeking to implement a consistent firm-wide cybersecurity program. Some firms may experience increased challenges if their branches may, for example, purchase their own assets, allow Bring Your Own Devices (BYOD), use nonapproved vendors, or not follow their firm's software patching and upgrade protocols. As a result, firms should evaluate whether they need to enhance their branch-focused cybersecurity measures to maintain robust cybersecurity controls and protect customer information across their organizations. Firms may want to consider asking the following questions, where applicable, with respect to how they supervise their branch network:

- What policies and procedures regarding cybersecurity and annual attestations of compliance have been established for each of your firm's branch offices?
- What cybersecurity training required when onboarding new branch locations or new staff?
- How does your firm confirm each of its branches meet firm cybersecurity standards, use firm-recommended vendors or other vendors meeting firm standards? What consequences does the firm impose (such as fines, sanctions or termination) on branches and registered representatives engaging in repeat violations of firm standards?
- What compliance and technology support does your firm provide its branches and registered representatives implementing firm cybersecurity protocols?
- What are your firm's configuration requirements for physical security and technical controls at each branch (*e.g.*, hard drive encryption, virus protection, MFA, patching and removable storage media)? How does your firm monitor these controls? Are these controls reviewed during branch inspections or monitored through the use of automated tools?
- How does your firm confirm that each of its branches use only secure, encrypted wireless settings for office and home networks?
- If a review of one of your firm's branches identifies material deficiencies or reported material cybersecurity incidents, how does it confirm that the branch has implemented corrective action?

7 INCIDENT MANAGEMENT AND RESPONSE

☐ Reviewed ✔

Incident response plans can help small firms address cybersecurity threats from bad actors. Developing and implementing an incident response plan may require contracting with an outside specialist but doing so may aid firms in responding to threats rapidly and effectively. Cybersecurity-related incidents may also require firms to file a SAR with the Financial Crimes Enforcement Network (FinCEN), as well as notify the FBI through their Internet Crime and Complaint Center (IC3) and the Federal Trade Commission (FTC). Firms may want to consider asking the following questions, where applicable, with respect to how they develop and implement their incident response plans:

- Does your firm maintain an incident response plan to identify and escalate incidents in a timely manner?
- Does your firm have the data inventory, assets inventory, and controls to assess the impact of incidents?
- Does your firm have capabilities for incident detection, containment, mitigation, and recovery either from internal resources or with help from a third party? If from a third party, have you established the relationship with defined service level agreements (SLAs)?
- What communication plans does your firm prepare for outreach to relevant stakeholders (*e.g.*, customers, regulators, law enforcement, intelligence agencies, industry information-sharing bodies) if an incident occurs?
- Do your firm's post incident reviews aim for improvements, including evaluating the incident management process, policy updates and control effectiveness?
- Have you tested the incident response plan within the past year?[7]
- Has the firm investigated or considered cybersecurity insurance?

8 TRAINING

☐ Reviewed ✔

A well-trained staff is an important defense against cyberattacks. Even well-intentioned staff can become inadvertent vectors for successful cyberattacks, so effective training helps reduce the likelihood that such attacks will be successful. Firms may want to consider asking the following questions, where applicable, with respect to how they design internal cybersecurity training, what personnel they require to take the training and how frequently they conduct and evaluate the training:

- How frequently and consistently does your firm conduct cybersecurity training? Are all individuals or third parties at the firm included in cybersecurity training? How often does your firm conduct training?
- Is your firm's training tailored to the cybersecurity risks applicable to its business? Does the training encompass a variety of methods (*e.g.,* reminder emails, online formal training, discussions of actual events)?
- Does your firm's training include simulated phishing exercises to validate employee understanding and track participation metrics? What consequences do employees face if they don't pass (*e.g.*, mandatory retraining)?
- How does your firm ensure that IT personnel are trained and kept abreast of the cybersecurity threat landscape to continuously assess the effectiveness of technical controls?
- Has your firm considered incorporating a formal or informal evaluation of the staff's understanding of and compliance with firm cybersecurity requirements into its training program?

[7] For additional guidance, *see* the NIST Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.

Appendix 1 – Glossary

Account Takeover (ATO) – a form of identity theft where a fraudster uses stolen login credentials to gain unauthorized access to another individual's online account.

Bring Your Own Device (BYOD) – a policy that allows firm employees to use their personal devices (*e.g.*, computers, smartphones, tablets) to access the firm's network.

Data Loss Prevention (DLP) – a set of technologies, products, and techniques that prevent end users from moving key information outside the firm's network.

Endpoint Detection and Response (EDR) Tools – integrated endpoint security solutions that combine real-time continuous monitoring and collection of endpoint data with rules-based automated responses and analysis capabilities.

Host-Based Intrusion Detection System (HIDS) and Host-Based Intrusion Prevention System (HIPS) – software that protects computer systems from malware and other unwanted, negative activity utilizing advanced behavioral analysis and the detection capabilities of network filtering to monitor running processes, files, and registry keys within an operation system.

Multi-Factor Authentication (MFA) – an authentication method that requires a user to provide two or more verification factors to gain access. Verification factors include something you know (password), something you have (token), something you are (biometrics), or somewhere you are (Geolocation).

Managed Service Providers (MSP) – third-party companies that remotely manage a customer's information technology (IT) infrastructure and end-user systems.

Managed Security Service Providers (MSSP) – providers of outsourced monitoring and management of security devices and systems, which may include security hardening, security monitoring, incident response and forensics services.

Personally Identifiable Information (PII) – data or information that allows the identity of an individual to be directly or indirectly inferred.

Principle of Least Privilege – the information security practice that any user, program or process should have the bare minimum privileges necessary to perform a function.

Service Level Agreement (SLA) – a contract between a service provider and a customer that identifies the types of provided services, and the standards the customer expects the service provider to meet.

Appendix 2 – Additional Resources

FINRA

Guidance

- *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* *20-30* (Fraudsters Using Registered Representatives Names to Establish Imposter Websites)
- *Regulatory Notice* *20-13* (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)
- *Regulatory Notice* *12-05* (Verification of Emailed Instructions to Transmit or Withdraw Assets From Customer Accounts)

Reports

- 2022 Report on FINRA's Examination and Risk Monitoring Program – Cybersecurity and Technology Governance
- Report on Selected Cybersecurity Practices – 2018
- Report on Cybersecurity Practices – 2015

Compliance Tools and Other Resources

- Compliance Vendor Directory
- Cybersecurity Topic Page
- Firm Checklist for Compromised Accounts
- Small Firm Cybersecurity Checklist

Non-FINRA Resources

- CIS: Critical Security Controls
- FBI: Internet Crime and Complaint Center (IC3)
- FinCEN: SAR Filing Instructions
- FTC: Cybersecurity for Small Business
- FTC: ReportFraud.ftc.gov
- NIST: Cybersecurity Framework
- NIST: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

FINRA Compliance Tool Disclaimer

This optional tool is provided to assist member firms in fulfilling their regulatory obligations. This tool is provided as a starting point, and you must tailor this tool to reflect the size and needs of your firm. Using this tool does not guarantee compliance with or create any safe harbor with respect to FINRA rules, the federal securities laws or state laws, or other applicable federal or state regulatory requirements. This tool does not create any new legal or regulatory obligations for firms or other entities.

Updates – This tool was last updated on May 5, 2022. This tool does not reflect any regulatory changes since that date. FINRA periodically reviews and update these tools. FINRA reminds member firms to stay apprised of new or amended laws, rules and regulations, and update their WSPs and compliance programs on an ongoing basis.

Member firms seeking additional guidance on certain regulatory obligations should review the relevant FINRA Topic Pages, including the Cybersecurity Topic Page.

Staff Contact(s) – FINRA's Office of General Counsel (OGC) staff provides broker-dealers, attorneys, registered representatives, investors and other interested parties with interpretative guidance relating to FINRA's rules. Please see Interpreting the Rules for more information.

OGC staff contacts:

Jeanette Wingler
FINRA, OGC
1735 K Street, NW
Washington, DC 20006

(202) 728-8000

Branch Office Inspections
Tuesday, May 17, 2022
4:15 p.m. – 5:15 p.m.

Join FINRA staff and industry panelists as they share how they implemented their remote branch inspection plan using Zoom, electronic documentation review and other technological tools. During the session, panelists discuss red flags, and how they prioritize their inspections.

Moderator:

Erin Vocke
Vice President, Retail Firm Examinations
FINRA Member Supervision

Panelists:

Brooks Brown
Senior Director, High Risk Registered Representative Program
FINRA Member Supervision

Samantha Larew
Chief Compliance Officer
Manning & Napier Investor Services, Inc.

Daniel Wright
First Vice President and Chief Compliance Officer
Cambridge Investment Research, Inc.

Branch Office Inspections Panelists Bios:

Moderator:

Erin C. Vocke is Vice President, Firm Group Examinations located in the New Orleans Office. Ms. Vocke began her career in 1995 as an examiner in the New Orleans District Office. During this time, she conducted routine and cause examinations of member firms and focused examinations in the areas of variable products and mutual funds. Ms. Vocke became Supervisor of Examiners and relocated to the Florida Office. She assumed responsibilities for supervising Continuing Membership Applications and financial surveillance of member firms, in addition to routine and cause examinations. Ms. Vocke was promoted to Associate District Director of the Dallas Office and assumed responsibility of overseeing the District cycle, cause, financial surveillance and Membership Application Programs. She served as the District Director of the Dallas District Office for approximately five years and the District Director for both the Dallas and New Orleans District Offices for approximately six years. In her new role, she will be responsible for examinations of retail member firms across Member Supervision.

Panelists:

Brooks Brown is Senior Director, National Cause and Financial Crimes in FINRA's Atlanta Office. Mr. Brown has been with FINRA since 2001 and currently oversees the High-Risk Representative Program. Mr. Brown is responsible for directing the identification and examination efforts related to registered representatives exhibiting elevated risk to investors. Previously, Mr. Brown served as an Associate District Director and Examination Manager as part of the Atlanta Office's firm examination program, overseeing examiners who conducted cycle examinations for compliance with FINRA and SEC rules. Prior to joining FINRA, Mr. Brown worked with Trustmark National Bank in Jackson, Mississippi as an equity analyst in Trustmark's Trust Department. Mr. Brown is a graduate of Millsaps College in Jackson, Mississippi, and has a Master of Business Administration Degree from Millsaps College's Else School of Management. Mr. Brown also earned the Certified Regulatory and Compliance Professional designation from the Wharton School in 2013.

Samantha Larew is Chief Compliance Officer and AML Compliance Officer for Manning & Napier Investor Services, Inc., a mutual fund distributor and retailer, located in Fairport, New York. Ms. Larew also serves as Chief Compliance Officer and AML Compliance Officer for the Manning & Napier Fund, Inc. Ms. Larew has over 17 years of experience in the financial services industry, 15 of which have been with Manning & Napier. As CCO for a broker-dealer and registered investment company she oversees all aspects of regulatory compliance, including the development and maintenance of Compliance Programs, branch office inspections, AML policies and procedures, and sales practice supervision, among other matters. As co-Director of Compliance, Ms. Larew supervises a team of four who conduct day-to-day compliance and supervision functions such as licensing and registration, advertising reviews, and regulatory gap analysis. Most importantly, across her roles, Ms. Larew focuses on building a strong culture of compliance and fostering positive and lasting working relationships with the business. Ms. Larew earned her BS in Political Science from the State University of New York College at Brockport. She currently holds FINRA's Certified Regulatory and Compliance Professional (CRCP)® designation, along with the Series 6, 7, 24, 26, 63, and 66 licenses. Additionally, Ms. Larew is presently serving on the FINRA North Region Committee.

Daniel Wright joined Cambridge in 2020 and has more than 25 years of experience in the financial services industry, with a background in compliance and operations. In his current role as First Vice President of Compliance and Chief Compliance Officer, Mr. Wright provides compliance oversight for Cambridge's broker-dealer activities while identifying and working to mitigate potential risks for the firm and its independent financial professionals. He is also responsible for implementing the firm's broker-dealer compliance policies and ensuring the firm complies with all applicable rules and regulations. Mr. Wright earned a Bachelor of Arts degree from

Oklahoma State University. He is a Certified Regulatory and Compliance Professional (CRCP)®. Additionally, he holds the FINRA Series 4, 7, 8, 24, 27, 53, 57,63, 65, and 99 licenses.

Branch Office Inspections

Panelists

- **Moderator**
  - Erin Vocke, Vice President, Retail Firm Examinations, FINRA Member Supervision
- **Panelists**
  - Brooks Brown, Senior Director, High Risk Registered Representative Program, FINRA Member Supervision
  - Samantha Larew, Chief Compliance Officer, Manning & Napier Investor Services, Inc.
  - Daniel Wright, First Vice President and Chief Compliance Officer, Cambridge Investment Research, Inc.

To Access Polling

- **Please get your devices out:**
  - Type the polling address, **https://finra.cnf.io/sessions/z1bf** into the browser or scan the QR code with your camera.

  - Select your polling answers.

Agenda

- Introduction
- Key Techniques and Lessons Learned
- Identifying “Red Flags” of Misconduct
- Technology Used in Branch Inspections
- Case Examples
- Q & A

1 | Introduction

Polling Question 1

1. **For 2022, what percentage of your branch inspections do you anticipate will be conducted on-site?**
   a. Less than 25%
   b. 25% to 50%
   c. 50% to 75%
   d. 75% to 100%

Polling address: **https://finra.cnf.io/sessions/z1bf**

2 | Key Techniques and Lessons Learned

3 | Identifying “Red Flags” of Misconduct

4 | Technology Used in Branch Inspections

5 | Case Examples

6 | Q & A

Branch Office Inspections
Tuesday, May 17, 2022
4:15 p.m. – 5:15 p.m.

Resources:

- FINRA *Regulatory Notice 20-16, FINRA Shares Practices Implemented by Firms to Transition to, and Supervise in, a Remote Work Environment During the COVID-19 Pandemic* (May 2020)

  www.finra.org/rules-guidance/notices/20-16

- FINRA *Regulatory Notice 20-13, FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic* (May 2020)

  www.finra.org/rules-guidance/notices/20-13

- FINRA *Regulatory Notice 20-08, Pandemic-Related Business Continuity Planning, Guidance and Regulatory Relief* (March 2020)

  www.finra.org/rules-guidance/notices/20-08

- FINRA *Regulatory Notice 17-38, FINRA Requests Comment on a Proposal to Amend Rule 3110 (Supervision) to Provide Firms the Option to Conduct Remote Inspections of Offices and Locations That Meet Specified Criteria Comment Period* (November 2017)

  www.finra.org/rules-guidance/notices/17-38

- 2022 Report on FINRA's Examination and Risk Monitoring Program

  www.finra.org/sites/default/files/2022-02/2022-report-finras-examination-risk-monitoring-program.pdf

- 2021 Report on FINRA's Examination and Risk Monitoring Program

  www.finra.org/sites/default/files/2021-02/2021-report-finras-examination-risk-monitoring-program.pdf

- FINRA Proposed Rule Change to Extend the Effectiveness of Temporary FINRA Rule 3110.17 to December 31, 2022

  www.finra.org/rules-guidance/rule-filings/sr-finra-2022-001#:~:text=The%20proposed%%20additional20six%2Dmonth,component%20of%20Rule%203110(c

- FINRA Rule change to extend temporary Supplementary Material .17 (Temporary Relief to Allow Remote Inspections for Calendar Years 2020 and 2021, and Through June 30 of Calendar Year 2022) under FINRA Rule 3110 (Supervision) to include calendar year 2022 inspection obligations through December 31, 2022 within the scope of the supplementary material.

  www.tools.finra.org/rule_filings/#:~:text=Details-,SR%2DFINRA%2D2022%2D001,-Rule%20change%20to

