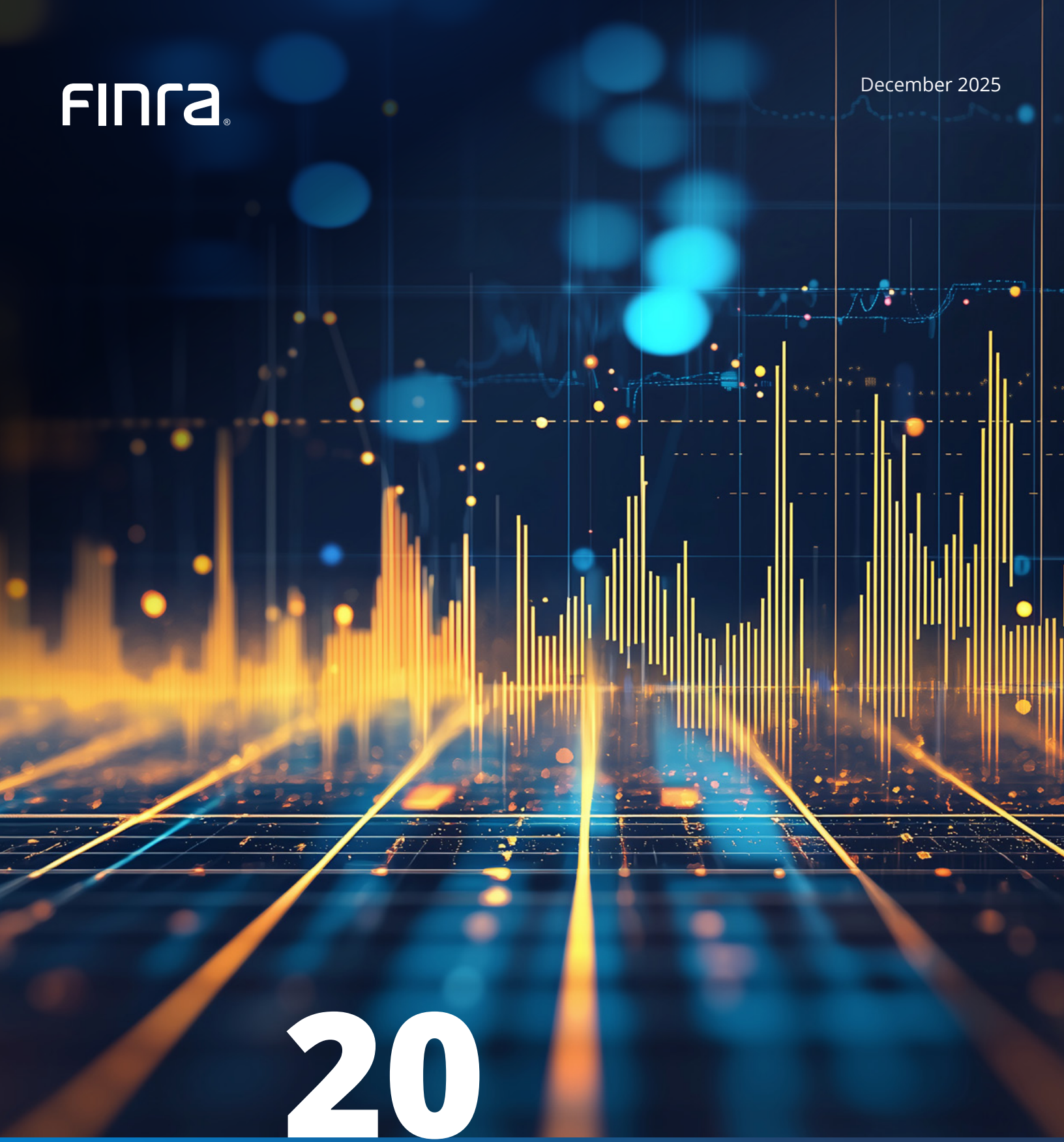
FINRA

December 2025



# 2026 FINRA ANNUAL REGULATORY OVERSIGHT REPORT

# Table of Contents

# Message From the Chief Regulatory Operations Officer

FINRA's mission to protect investors and promote market integrity drives everything we do, including our commitment to transparency and collaboration with our member firms. Whenever possible, we share actionable insights from our oversight activities to help firms enhance their resiliency and strengthen their compliance programs. Of all the publications we deliver, this **Annual Regulatory Oversight Report** is the most anticipated, with the greatest engagement of any of our resources. This year we have worked to publish the Report even earlier, in response to feedback from our members, who have told us what a valued resource it is for their annual compliance planning. The 2026 Report includes new and updated content on cyber-enabled fraud, senior investors and trends in generative artificial intelligence (GenAI), among other topics. These insights from our oversight activities—combined with other intelligence—are designed to help member firms identify emerging risks and implement effective controls as needed.

This year's Report also highlights progress on our **FINRA Forward** initiative, launched this spring. A key tenet of FINRA Forward is empowering member firm compliance. This includes offering more conferences, events and other tools; it also means strengthening the feedback loop from FINRA's regulatory programs to our member firms. That is a key goal of this Report: by sharing intelligence about key risks and emerging challenges, we can help our members enhance their compliance capabilities and proactively address potential issues before they become compliance failures.

FINRA Forward also reflects our commitment to continuous organizational improvement. This has included reviewing and enhancing our organizational structure to align to the demands of our mission, including integrating our core regulatory programs into a unified Regulatory Operations function. This integration will support more effective collaboration across our regulatory programs, resulting in more coordinated interactions with our member firms, expanded intelligence sharing across departments, more integrated processes and technology, and enhanced capacity to respond to the ever-evolving risks to investors and markets. The continuing integration of FINRA's regulatory programs is reflected in the Report, which draws on insights from across the Member Supervision, Market Oversight (formerly Market Regulation) and Enforcement teams.

We value your feedback on how we can improve the Report to make it more useful for our members. Please share your thoughts and suggestions with the Office of Strategic Engagement.

Sincerely,

*Greg Ruppert*

# Introduction

The 2026 FINRA Annual Regulatory Oversight Report (the "Report") provides FINRA member firms ("firms") with insight into findings from FINRA's regulatory operations programs. The Report reflects FINRA's commitment to providing transparency to firms and the public about our regulatory observations and activities.

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 prior Reports by adding new topics denoted **NEW FOR 2026** and new material (*e.g.*, new findings, effective practices) to existing sections where appropriate. (New material is in **bold** type.)

This year's Report addresses a broad range of content, including a new topic area dedicated to GenAI: Continuing and Emerging Trends.

Additionally, the Report highlights new content on various topics denoted in blue "callout" boxes, including updates on:

- FINRA Forward – Enhancing FINRA's Capabilities in an Evolving Industry;
- Increase in Small-Cap Fraud Involving Exchange-Listed Equities; and
- Annual Financial Reporting Reminders and Updates for Member Firms.

Please note that the removal of a topic or content from this year's Report does not indicate that the topic is not of regulatory importance, and you may find it helpful to continue to review those topics and content in the previous Reports as well as other guidance and tools available on FINRA.org.

For each topic area covered, the Report continues to:

- identify the relevant rule(s);
- summarize noteworthy findings from recent oversight activities involving firms;
- outline firms' effective practices that FINRA observed through its oversight activities; and
- provide additional resources that may be helpful to firms in reviewing their supervisory procedures and controls and fulfilling their compliance obligations.

FINRA welcomes feedback on how we can improve future publications of this Report. Please contact the Office of Strategic Engagement to provide recommendations.

## HOW TO USE THIS REPORT

We selected the topics in this Report for their interest to the largest number of firms; consequently, they may include areas that are not relevant to an individual firm and omit other areas that are applicable.

FINRA advises each firm to review the Report and consider incorporating relevant elements into its compliance program in a manner tailored to the firm's activities and applicable regulatory requirements. The Report is intended to be just one of the tools a 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, findings, effective practices or topics that FINRA will examine.

FINRA also reminds firms to stay apprised of new or amended laws, rules and regulations, and update their written supervisory procedures (WSPs) and compliance programs in response. Firms may contact their Risk Monitoring Analyst if they have any questions about the findings or effective practices included in this Report.

The Report contains the following, as applicable, for each topic area:

### Regulatory Obligations

A brief description of relevant federal securities laws, regulations and FINRA rules.

### Findings

Select findings from recent reviews, examinations, market surveillance, investigations or enforcement activities involving firms; or such findings from prior Reports that we continue to note in recent oversight activities.

### Effective Practices

Some select firms' practices that FINRA has observed through our oversight activities, which may help firms in tailoring their compliance programs depending on their business model, size and practice.

### Additional Resources

A list of relevant FINRA *Regulatory Notices*, other reports, tools and online resources.

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

As a reminder, the Report—as with our previous Exam and Risk Monitoring Reports, Findings Reports and Priorities Letters—does not create any new legal or regulatory requirements or new interpretations of existing requirements, or relieve firms of any existing obligations under federal securities laws and regulations. Readers should not infer that FINRA requires firms to implement any specific practices described in this Report that extend beyond the requirements of existing federal securities provisions or FINRA rules. Rather, firms may consider the information in this Report in developing new, or modifying existing, compliance practices. Moreover, some content may not be relevant to individual firms based on their business models, size or practices.

## FINRA Forward – Enhancing FINRA's Capabilities in an Evolving Industry

In spring 2025, FINRA launched FINRA Forward—a series of initiatives to enhance our efficiency and effectiveness in pursuit of FINRA's mission of protecting investors and safeguarding market integrity. The goal of this comprehensive effort is to evolve FINRA's capabilities and keep pace with the rapidly changing securities industry and markets, supporting vibrant capital markets in which everyone can invest with confidence.

Among the initiatives comprising FINRA Forward are efforts to:

- *modernize FINRA rules* via a broad review to modernize requirements, facilitate innovation and eliminate unnecessary burdens;
- *empower member firm compliance* by enhancing FINRA's support for member firm compliance programs; and
- *combat risks related to cybersecurity and fraud* by expanding FINRA's cybersecurity and fraud prevention activities to support member firms' risk management capabilities and resilience against emerging threats.

Upon the launch of FINRA Forward, FINRA published a series of *Regulatory Notices*:

- *25-04* on the broad review of FINRA's regulatory requirements;
- *25-05* on outside activities requirements;
- *25-06* on promoting capital formation; and
- *25-07* on the modern workplace.

To allow for member firm engagement and for the fulfillment of the robust rulemaking process, many of the rule changes FINRA adopts in response to FINRA Forward may happen over time. However, in many ways the contents of the 2026 Report reflect FINRA's efforts toward the initiative, from extensive updates and added resources in the Cybersecurity and Cyber-Enabled Fraud and Anti-Money Laundering, Fraud and Sanctions sections, to the new GenAI topic.

The Report reinforces FINRA's commitment to providing transparency to member firms about its regulatory observations and activities to help firms strengthen their compliance programs.

### Additional Resources

- FINRA Forward
- FINRA Crypto and Blockchain Education Program
- FINRA Blog Post: New FINRA Initiatives to Support Members, Markets, and the Investors They Serve
- FINRA Unscripted: Building Cybersecurity Resilience Through FINRA Forward
- FINRA Cyber & Operational REsilience (CORE)

# Financial Crimes Prevention

## CYBERSECURITY AND CYBER-ENABLED FRAUD

### Regulatory Obligations

Cybersecurity incidents may expose firms to loss of customer information, financial losses, reputational risks and operational failures. The failure to have a well-designed cybersecurity program could result in compliance shortfalls. Rules and regulations that may be implicated in the cybersecurity space include SEC Regulations S-P (Privacy of Consumer Financial Information and Safeguarding Personal Information) and S-ID (Identity Theft Red Flags), as well as FINRA Rules 3110 (Supervision) and 4370 (Business Continuity Plans and Emergency Contact Information), and Securities Exchange Act (SEA) Rules 17a-3 and 17a-4.

Rule 30 of SEC Regulation S-P requires member firms to, among other things, have written policies and procedures that address administrative, technical and physical safeguards for the protection of customer information.[1] Regulation S-ID requires member firms that offer or maintain one or more covered accounts[2] to develop and implement a written program that is designed to detect, prevent and mitigate identity theft in connection with the opening or maintenance of such accounts.[3]

#### Amendments to Regulation S-P

In May 2024, the SEC announced the adoption of amendments to Regulation S-P. The amendments provide, among other things, that a firm's policies and procedures to safeguard customer information must include a program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including procedures to notify affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.

Larger entities were required to comply with the amendments to Regulation S-P by Dec. 3, 2025. Smaller entities must comply with the amendments by June 3, 2026.

### FINRA has observed a variety of sophisticated cybersecurity threats targeting member firms and their customers, including:

- *Ransomware and Extortion Events:* cyberattacks involving unauthorized access to firm systems, often installing malware to encrypt or access and steal sensitive firm data or customer information. The stolen or encrypted data is held for ransom;
- *Data Breaches:* unauthorized access, acquisition or disclosure of confidential information, such as firm data and customer data, including personally identifiable information (PII);
- *Phishing,*[4] *Smishing*[5] *or Quishing:*[6] deceptive social engineering attacks using email, SMS text messages or QR codes to redirect customers to malicious domains for the purposes of gathering their login and other credentials;
- *New Account Fraud:* attacks using falsified customer information or stolen identity information often purchased from criminal sites on the dark web, via a mobile app or internet browser, for the purpose of opening accounts;
- *Account Takeovers*: threat actors using compromised customer login credentials to gain unauthorized access to online accounts;
- *Account Impersonations:* threat actors using stolen customer information in combination with a compromised or spoofed email address to initiate actions, often a third-party wire transfer request, from the customer's account;
- *Imposter Sites:* attacks leveraging spoofed domains and social media profiles (including those that impersonate financial firms, registered representatives and FINRA staff) to defraud firms and customers;
- *Relationship Investment Scams:* deceptive schemes targeting customers directly through social media or through text messages, establishing trust and then defrauding their victims; and
- *Insider Threats:* incidents involving firm employees who purposely or inadvertently use their access to firms' systems to cause harm to firms and their customers.

### Through a variety of partnerships, FINRA is also aware of the following emerging cyber threats potentially posing threats to firms:

- *GenAI-Enabled Fraud:* threat actors exploiting GenAI's ease of use and wide range of applications to enhance their cyber-enabled crimes, for example, by:
  - generating fake content (*e.g.*, imposter sites, false identification documents, deepfake audio and video);
  - creating polymorphic malware, which is a type of malicious software that constantly morphs, evolves or changes appearance to avoid detection by security products; and
  - leveraging GenAI models to develop malicious tools, allowing those without technical ability to become sophisticated cybercriminals.

*Continued on next page*

*Continued from previous page*

- *Cybercrime-as-a-Service:* criminals with technical expertise selling tools and services—including information stealers, phishing kits and ransomware—to less technical threat actors, allowing them to commit sophisticated cybercrimes.

For additional guidance concerning threat actors' manipulation of GenAI to gain access to financial accounts and create new accounts in the names of unsuspecting investors, please see the Continuing Risk: New Account Fraud and Account Takeovers "callout" box in the Anti-Money Laundering, Fraud and Sanctions topic.

## Effective Practices

- ***Monitor for Customer Account Takeovers:*** **Review unusual or suspicious activity such as wire requests to third-party accounts—including previously unused third parties—and suspicious login activity from unidentified browsers or locations to determine whether further action (*e.g.,* trading and fund restrictions on the accounts) is appropriate.**
- *Multi-Factor Authentication:* Use multi-factor authentication (MFA) for login access to the firm's systems, including email and operational systems accessed by associated persons, firm staff, contractors and customers.
- *Monitor for Imposter Domains or Accounts:*
  - Monitor the internet (*e.g.,* through a domain name service (DNS) monitoring service) for any newly created imposter domains fraudulently representing the firm or a registered representative.
  - Monitor social media for accounts impersonating firm personnel.
  - Maintain written procedures for responding to reports of imposter domains or social media accounts.
- *Monitor Outbound Email:* Scan outbound email and attachments to identify and block exfiltration of sensitive customer information or confidential firm data.
- ***BYOD Program:*** **Establish reasonable supervision for associated persons, firm staff and registered representatives that establishes clear policies and procedures for secure use of "bring your own device (BYOD)."**
- ***Conduct Training and Security Awareness:*** **Regularly train staff on cybersecurity measures, including how to identify and report phishing or social engineering attacks.**
- ***Identity Verification:*** **Review email addresses and verify signatures associated with third-party accounts if funds are requested to be sent to or from those outside accounts.**
- *Conduct Tabletop Exercises (TTXs):* Conduct TTXs with stakeholders to discuss cyber and technology threat management and incident response.
- *Segment Networks:* Subdivide networks into separate sections to limit threat actor movement laterally within a network.

- ***Cross-Team Communication:*** **Encourage cyber and information technology staff to coordinate with AML staff about cybersecurity concerns and report suspicious activity.**
- ***Monitor Third-Party Vendor Risk:*** **Monitor risk arising from relationships with vendors.**

### Additional Resources

- FINRA
  - 2025 Report—Third-Party Risk Landscape
  - 2024 Cybersecurity Conference
  - Cybersecurity Key Topics Page, including:
    - Small Firm Cybersecurity Checklist (Sept. 7, 2023)
    - Core Cybersecurity Threats and Effective Controls for Small Firms (May 5, 2022)
    - Cyber Workshops and Tabletop Exercises
  - File a Regulatory Tip
- SEC
  - Compliance Outreach on Regulation S-P
  - SEC Charges Three Individuals with Impersonating Financial Professionals in Fraud Scheme Targeting Retail Investors (Dec. 11, 2024)
  - SEC Adopts Rule Amendments to Regulation S-P to Enhance Protection of Customer Information (May 16, 2024)
  - Enhancements to Regulation S-P: A Small Entity Compliance Guide
- CISA
  - CISA Tabletop Exercise Packages
  - Free Cybersecurity Services and Tools
  - Stop Ransomware
- FinCEN
  - Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (Nov. 8, 2021)
  - Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime (Oct. 25, 2016)

## ANTI-MONEY LAUNDERING, FRAUD AND SANCTIONS

### Regulatory Obligations

The Bank Secrecy Act (BSA) is the common name for the collection of laws enacted in the United States to combat money laundering and terrorist financing. The purposes of the BSA include, among others, requiring certain reports or records that are highly useful in criminal, tax or regulatory investigations, risk assessments or proceedings; or intelligence or counterintelligence activities, including analysis, to protect against terrorism.[7]

FINRA Rule 3310 (Anti-Money Laundering Compliance Program) requires that each member develop and implement a written anti-money laundering (AML) program that is approved, in writing, by senior management and is reasonably designed to achieve and monitor the member's compliance with the BSA and its implementing regulations.[8]

**FINRA Rule 3310 sets forth minimum standards for a member's written AML compliance program, requiring firms to:**

- **establish and implement policies and procedures that can be reasonably expected to detect and cause reporting of suspicious transactions (3310(a));**
- **establish and implement policies, procedures and internal controls reasonably designed to achieve compliance with the BSA and its implementing regulations, including regulations relating to Customer Identification Programs and beneficial owner verification (3310(b));**
- **conduct independent testing for compliance each calendar year (or every two calendar years in some specialized cases) (3310(c));**
- **designate an individual or individuals responsible for implementing and monitoring the day-to-day operations and internal controls of the program (3310(d));**
- **provide ongoing training for appropriate personnel (3310(e)); and**
- **maintain risk-based procedures for conducting ongoing customer due diligence, including to understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile and conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, to maintain and update customer information (3310(f)).**

### Evolving Risk: External Fraud

According to the recent FBI Internet Crime Report, fraud represented the most reported losses tracked by the FBI's Internet Crime Complaint Center (IC3) again this year. FINRA also continues to observe the evolution of external fraud threats impacting investors, markets and member firms. FINRA has previously highlighted external fraud threats—such as fraudulent requests to the Automated Customer Account Transfer System (ACATS), fraudulent options trading, account takeovers (ATOs) and new account fraud (NAF)—as well as related effective practices.[9] In addition, threat actors are attempting to entice investors to withdraw funds from their securities accounts and send the funds to the threat actor as part of a fraudulent scheme.

The 2025 FINRA Annual Regulatory Oversight Report included examples of external fraud schemes targeting investors directly. Examples of updated trends in this space include:

- *Disaster-Related Scams:* Schemes in which fraudsters seek to exploit natural disasters or other events that commonly prompt large volumes of donations to commit fraud.[10]
- *Investment Club Scams:* These schemes, often associated with pump and dump or other forms of market abuse, continue to evolve. Bad actors associated with an investment club scam will post fraudulent social media advertisements—often using the likeness of well-known finance personalities or financial professionals unaffiliated with the scam—to direct victims to purported "investment clubs" on encrypted messaging applications, where victims are persuaded to purchase shares of low-

*Continued on next page*

*Continued from previous page*

volume and thinly traded securities (most commonly, shares of stock). When enough victims purchase the shares that are the target of the scheme, the price of the shares rise (the "pump"). Bad actors then sell their shares at a profit, causing the price to plummet and leaving the victims with losses (the "dump").[11]

- *Gold Bar Courier Scams:* In a Gold Bar Courier scam, a fraudster will instruct victims to liquidate assets in securities accounts and purchase precious metals, such as gold bars. The bad actors later convince victims to turn over the precious metals to couriers, sometimes impersonating government officials, under the guise of offering custody or safekeeping services.
- *Crypto Confidence Frauds:* In a crypto confidence fraud, bad actors befriend people to entice them to make crypto investments through phony apps and websites. The investments may start out slowly with small sums of money, but it is a scam aimed at stealing tens of thousands to millions of dollars.[12]
- *Mail Theft-Related Check Frauds:* In a mail theft-related check fraud, bad actors steal physical checks sent via mail, then alter or counterfeit those checks to make unauthorized withdrawals.

Firms may consider incorporating the following effective practices into their risk-based compliance programs to help detect and mitigate the threat posed by external fraud:

- Leveraging strong risk-based compliance—especially related to FINRA Rules 3110 (Supervision) as it relates to the transmittal of customer funds (*e.g.*, establishing reasonable risk-based criteria for determining the authenticity of transmittal instructions), and FINRA Rule 3310 (Anti-Money Laundering) as it relates to the reasonable detection, investigation and reporting of potentially suspicious transactions—to assist member firms in identifying red flags of external fraud targeting their investors.
- Providing educational material to associated persons and customers explaining how scams occur and providing resources for victimized customers (including those on FINRA's For Investors page and FINRA's Scam Prevention and Assistance Resource Key Topics page).
- Establishing effective communication channels between anti-money laundering and anti-fraud compliance programs to quickly detect and respond to red flags of external fraud.
- Relying on FINRA Rule 2165 (Financial Exploitation of Specified Adults) to place a temporary hold on a customer's securities transactions or disbursements where there is a reasonable belief of customer financial exploitation.[13]
- Emphasizing the importance of trusted contact persons and promoting effective practices in connection with FINRA Rule 4512 (Customer Account Information).[14]
- Contacting FINRA's Securities Helpline for assistance.

*Continued on next page*

*Continued from previous page*

- Developing response plans for situations where the firm identifies that a customer has been victimized, including:
  - notifying a customer's trusted contact person of any concerns;
  - for elder or vulnerable adults, notifying Adult Protective Services;
  - in addition to filing required suspicious activity reports (SARs), reporting the fraud to the appropriate regulatory (*e.g.*, FTC, SEC) and law enforcement agencies (*e.g.*, FBI, the customer's state's Attorney General's Consumer Protection Office and Crime Victim Coalition); and
  - engaging with the FBI's IC3 Recovery Asset Team via its Internet Crime Complaint Center to attempt to recall outgoing wire transactions.

For additional guidance concerning external fraud identification, mitigation and prevention, please see:

- The Senior Investors and Trusted Contact Persons topic in the 2025 Report
- FINRA Scam Prevention and Assistance Resource Key Topics page
- FINRA Securities Helpline for Seniors
- FINRA Investor Alert: Relationship Investment Scams (Sept. 10, 2024)
- FINRA Threat Intelligence Product: Protecting Vulnerable Adult and Senior Investors (May 2024)
- FINRA Foundation's Taking Action: An Advocate's Guide to Assisting Victims of Financial Fraud (2021)
- *Regulatory Notice* 20-30 (Fraudsters Using Registered Representatives' Names to Establish Imposter Websites)
- *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 Notices* 22-21 (FINRA Alerts Firms to Recent Trend in Fraudulent Transfers of Accounts Through ACATS) and 23-06 (FINRA Shares Effective Practices to Address Risks of Fraudulent Transfers of Accounts Through ACATS)

## Findings

- *Failing to Reasonably Detect and Investigate Red Flags and Report Suspicious Transactions:* Failing to establish and implement an AML program reasonably designed to detect and cause the reporting of suspicious transactions. This included:
  - failing to reasonably tailor an AML program, including the detection and investigation of red flags, as well as monitoring processes and tools, to the firm's business;
  - failing to establish and implement reasonably designed policies and procedures related to the detection and investigation of red flags of suspicious trading and money movement activity—**including suspicious activity in omnibus accounts;**
  - **not reasonably detecting and investigating red flags of potentially suspicious activity associated with small-cap public offerings as highlighted in *Regulatory Notice 22-25* (Heightened Threat of Fraud), including investments well beyond the stated net worth of the customer(s), investments made by multiple customers that exhibit red flags of being nominee accounts, and simultaneous or near simultaneous trading by seemingly unrelated accounts that lacks a business purpose or appears designed to artificially inflate the price of the security;**[15]
  - failing to commit sufficient **staff and resources to the AML program**, including following a **material** business expansion or **change in business, or where new threats are applicable to the member;**
  - **failing to establish and implement reasonably designed policies and procedures for escalating and reviewing red flags of suspicious activity detected by another team or department outside of the AML compliance program that may require the filing of a SAR (*e.g.,* cybersecurity events, account compromise, account takeovers);**
  - **failing to reasonably detect and consider red flags of identity theft, either at onboarding or during investigations of potentially suspicious activity; and**
  - **failing to reasonably detect and investigate red flags associated with inquiries about potentially suspicious transactions received from the member's clearing firm about an introduced customer.**[16]
- ***Failing to Reasonably Establish and Implement Policies and Procedures to Achieve Compliance With Customer Identification Program (CIP) and Customer Due Diligence (CDD):***
  - Not recognizing that certain relationships established with the firm to effect securities transactions are customer relationships (and, consequently, not conducting CIP or CDD as required).
  - ***Unreasonable Verification of Customer Identities:* Not establishing and implementing a reasonably designed CIP. For example, failing to collect required identifying information, and not reasonably verifying the identity of customers and beneficial owners of legal entity customers within a reasonable timeframe, especially in situations where red flags related to the customer's identity are present, including red flags of identity theft, red flags that the customer may be acting as agent for an undisclosed principal using a nominee account, and other red flags in customer due diligence and interactions with customers).**[17]

- Auto-approving the opening of customer accounts without reasonably verifying the identity of the customer within a reasonable timeframe despite red flags (*e.g.*, applicant provided a Social Security number that was not valid or was associated with the name of a different person, including a deceased individual).
- **Not reasonably detecting and investigating red flags, including situations where the stated business, occupation or financial resources of the customer are not commensurate with the type or level of activity of the customer, to reasonably determine whether to file a SAR or update the customer risk profile.**
- Failing to establish policies and procedures that can be reasonably expected to detect identity theft or synthetic identity fraud in connection with account opening **(*e.g.*, common identifying information across multiple seemingly unrelated accounts**).
- Not conducting initial and ongoing risk-based CDD to **reasonably** understand the nature and purpose of customer relationships to develop a customer risk profile, **identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.**

- *Inadequate Due Diligence on Correspondent Accounts of Foreign Financial Institutions:* Not reasonably conducting required due diligence on correspondent accounts the firm maintains for foreign financial institutions, including by failing to assess the money laundering risk posed by such correspondent accounts, and failing to apply risk-based procedures and controls to each correspondent account reasonably designed to detect and report known or suspected money laundering activity, including a periodic review of the correspondent account activity sufficient to determine consistency with information obtained about the type, purpose and anticipated activity of the account.
- *Inadequate Testing:*
  - Not providing for annual testing of the program on a calendar-year basis (or every two calendar years in specialized circumstances).
  - Not **ensuring that AML independent tests include a reasonably designed assessment of** critical aspects of the AML program (*e.g.*, suspicious activity detection and reporting), including **following a material business expansion or change in business,** or where new threats to the industry are applicable to the member.
  - Not **ensuring** that persons **performing the AML independent test have** the requisite independence and qualifications to perform the testing.
- ***Inadequate Training:* Not providing ongoing AML training to appropriate personnel that is tailored to the firm's business.**

### Continuing Risk: New Account Fraud and Account Takeovers

FINRA has observed continued fraudulent activity associated with NAF, which are accounts opened using stolen identities, and ATOs, where bad actors use stolen customer credentials to access an existing customer account. Fraudsters are increasingly using GenAI tools to gain access to financial accounts and create new accounts in the names of unsuspecting investors. For example, fraudsters are using GenAI to exploit identification (ID) verification processes and commit new account fraud and account takeovers in multiple ways, including:

- *Social Engineering*—This involves tricking or manipulating investors into giving away sensitive information or allowing remote access to their computer. Fraudsters might use GenAI to analyze social media activity to create highly personalized phishing emails that could lead investors to fraudulent websites embedded with malicious links.
- *Voice Clones*—With GenAI, fraudsters can create a credible-sounding imitation, or voice clone, of an investor. Using this voice clone, they might persuade the member firm to grant or change access to the investor's accounts.
- *Fake ID Documents*—Fraudsters can use GenAI to create convincing fake ID documents—such as driver's licenses, professional credentials or bank statements—that might also incorporate AI-generated images. They can use these documents to fraudulently open a new account or to take over an existing account.
- *Deepfake Selfies*—Some firms have incorporated requests for selfie photos and videos into their customer-verification process. Fraudsters can take images from customers' social media and use GenAI to create deepfakes to circumvent these types of security checks.

Some effective practices for firms to consider incorporating into their risk-based compliance programs to help mitigate the threat posed by this type of fraud include the following, especially for firms that offer fully online account opening services and rely on automated account opening or customer verification services:

- Inform customers about identity-theft protection services and periodically remind customers to change user login information, including passwords, particularly after known data breaches and leaks that expose consumer login credentials.
- Encourage customers who know their SSNs have been compromised to use credit-monitoring services and consider requesting a credit freeze.
- Train employees, especially those involved in customer onboarding, on the latest in AI capabilities and threats, and be on alert for repetitive patterns of behavior in the opening of multiple accounts that could be indicative of bots and bad actors.
- Perform additional verification or authentication when anomalies are detected in customer login attempts or when the customer engages in transactions that would

*Continued on next page*

*Continued from previous page*

not be expected from unusual locations or Internet Protocol (IP) addresses, which can include phone calls, likeness checks or use of multi-factor authentication.

- Prevent or limit outgoing transfers of funds from potentially compromised accounts—for example, if an account password or contact information has just been changed and the account user is attempting to make out-of-pattern or higher-risk transactions.
- If the firm identifies one attempt by a bad actor to open an account, look for accounts opened at around the same time with similar characteristics.
- Join industry, regulatory and law-enforcement anti-fraud networks, and subscribe to their mailing lists. Members of these networks can more quickly learn of new threats and how to counter them.

For additional guidance, FINRA recommends:

- Investor Insights: Protecting Your Investment Accounts From GenAI Fraud (January 2025)
- *Regulatory Notice* 21-18 (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts)
- Nacha's ACH Operations Bulletin #1-2023 Update to Sample Written Statement of Unauthorized Debit
- FINRA Fraud Spotlight Webinar: New Account Fraud

## Effective Practices

- *Reviewing Regulatory Updates:* Reviewing alerts, advisories, significant cases and other updates from FINRA, the SEC, FinCEN, OFAC, and other regulators and agencies, and **assessing the relevance of the information to the member's business and whether adjustments to the firm's risk-based AML compliance program are warranted.**
- ***Clear Delegation of AML Responsibilities and Effective Communication Channels:*** **Establishing clear delegation of AML-related responsibilities across individuals and business units that are in the best position to identify red flags of suspicious activity through written procedures and recurring cross-department communication. This may include specifying which individuals and business units are responsible for:**
  - **detecting account compromise, account takeovers and other potential cyber events;**
  - **identifying potential insider trading, market manipulation or other market abuse;**
  - **reasonably detecting and responding to red flags of potential identity theft as part of the member's Identity Theft Prevention Program as required under Regulation S-ID; and**
  - **detecting potentially fraudulent transmittals of funds or securities from customer accounts and using a reasonable risk-based criteria to determine the authenticity of transmittal instructions.**

- *Independent Testing:* **Comprehensive AML independent testing can identify areas of the member firm's AML Compliance Program that may be unreasonably designed or implemented, and provide members with the ability to take prompt corrective action that can mitigate the risk of illicit proceeds being laundered or generated by, at or through the firm.**
- *Training:* Establishing and maintaining an AML training program for appropriate personnel that is tailored to the individuals' roles and responsibilities, addresses AML risks **relevant to the member's business and recent** regulatory developments, and, where applicable, leverages trends and findings from the firm's quality assurance controls and AML independent testing.
- *Conducting Risk Assessments:*
  - Conducting AML risk assessments that are updated in appropriate situations, such as:
    - following material findings of an independent AML test or other internal or external audits;
    - following changes in the size or risk profile of the firm (*e.g.*, changes to business lines, products and services, registered representatives, customers or geographic areas in which the firm operates); or
    - following material macroeconomic or geopolitical events.
  - **Periodically assessing alerts or exception reports to confirm they are functioning as intended, reasonably detecting the suspicious activity the alert or report is designed to identify, and properly ingesting the required data.**
- *Additional Steps for Verifying Customers' Identities When Establishing Online Accounts:* Incorporating additional methods for verifying customer identities, for example:
  - **obtaining** both documentary (*e.g.,* driver licenses, government issued IDs) and non-documentary identifying information, or multiple forms of documentary information;
  - asking follow-up questions or requesting additional documents based on information from credit bureaus, credit reporting agencies or digital identity intelligence (*e.g.*, automobile and home purchases);
  - contracting third-party vendors to help verify the legitimacy of suspicious information in customer applications (*e.g.*, cross-referencing information across multiple third-party vendors);
  - validating identifying information that applicants provide through likeness checks;[18]
  - reviewing the IP address or other available geolocation data associated with:
    - new online account applications for consistency with the customer's home address; and
    - transfer requests (for consistency with locations from which the firm has previously received legitimate customer communications);
  - obtaining a copy of the account statement from the account slated to be transferred before sending an ACATS request;
  - for firms that initiate ACATS transfers (*i.e.*, delivering firms), sending notifications to account owners (*e.g.*, "push" notifications on mobile apps, emails, phone calls) or contacting any broker(s) assigned to the account or both;

- ensuring that any tools used for automated customer verification are reasonably designed to detect red flags of identity theft and synthetic identity fraud;
- limiting automated approval of multiple accounts for a single customer;
- reviewing account applications for common identifiers (*e.g.,* email address, phone number, physical address) present in other applications and in existing accounts, especially seemingly unrelated accounts; and
- reviewing account applications for use of temporary or fictitious email addresses (*e.g.,* @temporaryemail.org) or phone numbers (*e.g.,* 555-555-5555, 999-999-9999).

## Additional Resources

- FINRA
  - Anti-Money Laundering (AML) Key Topics Page
  - Anti-Money Laundering (AML) Template for Small Firms (Sept. 8, 2020)
  - Frequently Asked Questions (FAQ) regarding Anti Money Laundering (AML)
  - Industry Risks and Threats – Resources for Member Firms
  - Identity Theft Red Flags Rule Template
  - *Regulatory Notices*
    - *Regulatory Notice* 22-25 (Heightened Threat of Fraud)
    - *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
  - Investor Alert: Beware of Fraudsters Impersonating Investment Professionals and Firms (Dec. 11, 2024)
  - Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities (Oct. 17, 2023)
  - Risk Alert: Observations from Anti-Money Laundering Compliance Examinations of Broker-Dealers (July 31, 2023)
  - Risk Alert: Observations from Broker-Dealer and Investment Adviser Compliance Examinations Related to Prevention of Identity Theft Under Regulation S-ID (Dec. 5, 2022)
  - Anti-Money Laundering (AML) Source Tool for Broker-Dealers (May 16, 2022)
  - Risk Alert: Compliance Issues Related to Suspicious Activity Monitoring and Reporting at Broker-Dealers (March 29, 2021)
- Treasury and FinCEN
  - **Frequently Asked Questions Regarding Suspicious Activity Reporting Requirements (Oct. 9, 2025)**
  - **FinCEN Alerts/Advisories/Notices/ Bulletins/Fact Sheets, including:**
    - **Financial Action Task Force Identifies Jurisdictions with Anti-Money Laundering, Countering the Financing of Terrorism, and Counter-Proliferation Finance Deficiencies (June 23, 2025)**
    - **FinCEN Reminds Financial Institutions to Remain Vigilant Regarding Potential Relationship Investment Scams (Feb. 26, 2025)**

- FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions (Nov. 13, 2024)
- FinCEN Notice on the Use of Counterfeit U.S. Passport Cards to Perpetrate Identity Theft and Fraud Schemes at Financial Institutions (April 15, 2024)
- FinCEN Alert to Financial Institutions to Counter Financing to Hamas and its Terrorist Activities (Oct. 20, 2023)
- FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering" (Sept. 8, 2023)

- **2024 National Money Laundering Risk Assessment**
- The Anti-Money Laundering Act of 2020 (June 30, 2021)
- Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (June 30, 2021)

- Financial Action Task Force
  - Risk-based Approach Guidance for the Securities Sector (Oct. 26, 2018)

## MANIPULATIVE TRADING

### Regulatory Obligations

Several FINRA rules prohibit firms from engaging in impermissible trading practices, including manipulative trading—for example, FINRA Rules 2010 (Standards of Commercial Honor and Principles of Trade), 2020 (Use of Manipulative, Deceptive or Other Fraudulent Devices), 5210 (Publication of Transactions and Quotations), 5220 (Offers at Stated Prices), 5230 (Payments Involving Publications that Influence the Market Price of a Security), 5240 (Anti-Intimidation/Coordination), 5270 (Front Running of Block Transactions), 5290 (Order Entry and Execution Practices) and 6140 (Other Trading Practices).

Under FINRA Rule 3110 (Supervision), firms are required to include in their supervisory procedures a process to review securities transactions that is reasonably designed to identify trades that may violate the provisions of the Exchange Act, the rules thereunder, or FINRA rules prohibiting insider trading and manipulative and deceptive devices that are effected for accounts of the firm and its associated persons. The firm must promptly conduct an internal investigation into any such trade to determine whether a violation of those laws or rules has occurred.

Among other obligations, FINRA Rule 5210 prohibits firms from publishing or circulating communications regarding transactions and quotations unless they believe the information is bona fide; FINRA Rule 5270 prohibits trading in a security or related financial instrument that is the subject of an imminent customer block transaction while in possession of material, non-public market information concerning that transaction; and FINRA Rule 6140 contains several requirements to ensure the promptness, accuracy, and completeness of last sale information for National Market System (NMS) stocks and to prevent that information from being publicly trade reported in a fraudulent or manipulative manner.

## Findings

- *Inadequate WSPs:*
  - Not having procedures reasonably designed—based on the types of business the firm engages in—to identify patterns of manipulative conduct; not identifying specific steps and individuals responsible for monitoring for manipulative conduct; and not outlining escalation processes for detected manipulative conduct.
  - Not tailoring procedures to reasonably supervise differing sources of order flow (*e.g.*, proprietary trades, retail customers, institutional customers, foreign financial institutions).
  - Not considering red flags from external sources (*e.g.*, inquiries from regulators, trading platforms, or other service providers or publicly available information about known manipulators).
- *Surveillance Deficiencies:*
  - Not establishing and maintaining a surveillance system reasonably designed to monitor for different types of manipulative trading schemes (*e.g.,* potential layering, spoofing, wash trades, prearranged trades, marking the close, odd-lot manipulation) with parameters that are reasonably designed and documented.
  - Not reasonably designing and establishing surveillance controls and thresholds to capture manipulative trading (*e.g.*, thresholds not designed to capture the appropriate market class of securities or type of securities or include both customer and proprietary trading or thresholds set too low or too high to identify meaningful activity).
  - Failing to periodically evaluate the adequacy of firms' surveillance controls and thresholds in light of changes in their business, customer base or the market.
  - Not adequately monitoring customer activity for patterns of potential manipulation (*e.g*., potential prearranged trading across customers), **including reviews that do not take into consideration patterns across appropriate lengths of time (*e.g.*, several days) or across different customers, or different alert types (*e.g.*, alerts for marking the close, matched trading, spoofing and layering).**
  - Not performing timely reviews of surveillance alerts or exception reports.
  - Not dedicating sufficient resources and training to reviews of surveillance alerts or exception reports.
  - Not documenting alert review findings.

### Increase in Small-Cap Fraud Involving Exchange-Listed Equities

In the 2025 FINRA Annual Regulatory Oversight Report and in *Regulatory Notice 22-25* (Heightened Threat of Fraud), FINRA reported that certain small-cap, exchange-listed issuers were being targeted for manipulative pump-and-dump schemes in connection with Initial Public Offerings (IPOs). These schemes primarily involved low-priced exchange-listed issuers with operations in foreign jurisdictions, and the IPOs typically offered a low amount of the issuers' public float for distribution in the IPO.[19]

In 2024 and 2025, these schemes have continued and evolved:

- FINRA continues to observe suspected pump-and-dump schemes occurring less frequently at the time of the small-cap issuers' IPOs, and more frequently months after these IPOs. Oftentimes, the same issuer is subject to multiple suspected pump-and-dump schemes.
- Suspected nominee accounts continue to be utilized to invest in small-cap IPOs to aid in bringing companies public. The suspected nominee accounts are typically centrally controlled by one or more bad actors that fund the accounts and control the activity in the accounts, sometimes remotely.
- In advance of the pump-and-dump scheme, nominee accounts may "funnel," or sell their shares in a coordinated manner to one or more foreign omnibus accounts, that result in the omnibus account(s) holding a significant portion of the public float.
- Similarly, well after the issuer's IPO, the issuer may sell a large amount of shares in a privately placed secondary offering to select foreign investors—lacking adequate public disclosure—leading to these investors holding a large amount of the issuer's public float. The shares are subsequently deposited at U.S. brokerage firms, or at foreign financial institutions that maintain accounts at U.S. brokerage firms.
- FINRA has also observed a new trend involving the use of account takeover (ATO) fraud to purchase shares of small-cap companies that are the subject of pump-and-dump schemes. After a bad actor accesses the account, the bad actor sells legitimately acquired investments and uses the funds to purchase shares of the subject securities.
- FINRA has observed a continued increase in the use of text messaging and social media-based scams to attract victims to purchase shares of small-cap issuers subject to pump-and-dump schemes. These include continued use of investment club scams, in which bad actors invite victims into social media-based investment clubs, directing victims on the time and price to buy certain small-cap securities.
- The victims' purchases occur in conjunction with—and likely cause—price increases in the targeted securities through the use of coordinated limit orders. These purchases often coincide with liquidations of shares by accounts presumed to be controlled by foreign bad actors, allowing the bad actors to profit from the schemes.

*Continued on next page*

*Continued from previous page*

In October 2025, FINRA initiated a targeted examination of firm practices regarding public and private offerings of small-cap, exchange-listed issuers with business operations in foreign jurisdictions.

For additional guidance, FINRA recommends these *Investor Insights* articles:

- Investor Insights: Avoiding Pump-and-Dump Scams (April 24, 2025)
- Investor Alert: Social Media 'Investment Group' Imposter Scams on the Rise (Jan. 11, 2024)
- Investor Insights: This On-Ramp Could Lead You to a Dump (March 30, 2023)

Also see the Anti-Money Laundering, Fraud and Sanctions topic.

## Effective Practices

- *Manipulative Schemes:*
  - Tailoring **surveillance control parameters and thresholds** and processes designed to detect different types of manipulative order entry and trading activity based on product class, including listed and OTC equities, options and fixed income products (*e.g.*, Treasuries).
  - Monitoring for red flags associated with customer accounts that may have a relationship with an issuer, such as:
    - customer accounts (foreign or domestic) referred by a small-cap issuer to the underwriting broker-dealer (particularly when the same officer or CEO has been noted across multiple issuers); and
    - money movements between the issuer and customer accounts.
  - Monitoring for red flags indicating:
    - conflicts of interest in private capital raises in advance of IPOs (particularly where a nominee controls shares); and
    - the involvement and participation in underwriting and selling activities by unregistered individuals in private and public offerings.
  - Supervising for efforts by the firm or customers to artificially support or suppress the price, or prevent or reduce natural price falls, of securities.
- *Multiple Platform and Product Monitoring:* Monitoring activity occurring across multiple platforms, including platforms that **support trading in** related financial instruments or correlated products, as well as cross-border activity in the same or related products.
- *Exchange-Traded Products (ETPs):* Developing and maintaining a robust supervisory system to safeguard material, non-public information to prevent front running and trading ahead by:
  - establishing effective information barriers and controls to prevent information leakage and the misuse of material, non-public information;

- reviewing for manipulative strategies that exploit the unique characteristics of ETPs (*e.g.*, their creation and redemption processes) and strategies that exploit information leakage related to portfolio composition files (including those associated with rebalancing events); and
- tailoring the firm's compliance program to align with how the firm trades ETPs.

- *Wash and Prearranged Trading:* Monitoring activity to identify firm customers engaging in wash trading (*e.g.*, to collect liquidity rebates from exchanges) or prearranged trading (*e.g.*, to create the appearance of active trading), by:
  - monitoring accounts identified as related (or in concert) in the firm's wash/prearranged trading surveillance reports; and
  - reviewing trading activity that relates to information provided on account opening documents.

## Additional Resources

- FINRA
  - *Regulatory Notice* 22-25 (Heightened Threat of Fraud: FINRA Alerts Firms to Recent Trend in Small Capitalization IPOs)
  - *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)
  - *Regulatory Notice* 18-25 (FINRA Reminds Alternative Trading Systems of Their Obligations to Supervise Activity on Their Platforms)
  - *Regulatory Notice* 17-22 (FINRA Adopts Rules on Disruptive Quoting and Trading Activity and Expedited Proceedings)

# GenAI: Continuing and Emerging Trends – NEW FOR 2026

## Regulatory Obligations

FINRA's rules—which are intended to be technologically neutral—and the securities laws more generally, continue to apply when firms use GenAI or similar technologies in the course of their businesses, just as they apply when firms use any other technology or tool. It is important for firms to consider how they will comply with applicable regulations, including FINRA rules, when evaluating GenAI tools prior to testing and deployment within their business environment.

For example, using GenAI can implicate rules regarding supervision, communications, recordkeeping and fair dealing. Pursuant to FINRA Rule 3110 (Supervision), a member firm must have a reasonably designed supervisory system tailored to its business. If a firm is relying on Gen AI tools as part of its supervisory system, its policies and procedures may consider the integrity, reliability and accuracy of the AI model.

## HOW FINRA MEMBER FIRMS USE GenAI

Generative AI (GenAI) use cases are emerging quickly in the financial industry. This use portfolio reflects some of the most common GenAI use cases FINRA has observed among our member firms. We are sharing how we categorize and define these uses, as it may be helpful to our fellow regulators, member firms, and others to have a shared terminology to facilitate discussions of this fast-evolving technology.

### Use Case Types

**Summarization & Information Extraction**
Condensing large volumes of text and extracting specific entities, relationships, or key information from unstructured documents

**Conversational AI & Question Answering**
Providing interactive, natural language responses to user queries through chatbots, virtual assistants, and voice interfaces

**Sentiment Analysis**
Assess the tone of the text as positive, neutral, or negative

**Translation**
Translating text between supported languages, convert audio to text or vice versa

**Content Generation & Drafting**
Creating a variety of written content, including documents, reports, marketing materials, and other resources

**Classification & Categorization**
Automatically sorting, labeling, and organizing data, documents, or transactions into predefined categories or groups

**Workflow Automation & Process Intelligence**
Optimizing business processes through intelligent routing, automation, and agents

**Coding**
Generating functional code for specified inputs and output objectives

**Query**
Retrieving results from structured databases with natural language

**Synthetic Data Generation**
Refers to the process of creating artificial datasets that resemble real-world data but are generated by computer algorithms or models rather than being collected from actual observations or measurements

**Personalization & Recommendation**
Tailoring products, services, or content to customer preferences and circumstances

**Analysis & Pattern Recognition**
Identifying trends, correlations, or anomalies in complex datasets to generate insights and predictions. Including the identification of threat activity of adversaries

**Data Transformation**
Converting unstructured data into standardized formats

**Modeling & Simulation**
Automation of financial modeling, forecasting, scenario creation, and simulations

## EMERGING TRENDS AND CURRENT PRACTICES

Through FINRA's survey of firms and engagement with other regulators, FINRA has noted that:

- firms have started to implement GenAI solutions with a focus on efficiency gains, particularly with respect to internal processes and information retrieval; and
- the top GenAI use case among FINRA member firms is "Summarization and Information Extraction," which refers to condensing large volumes of text and extracting specific entities, relationships or key information from unstructured documents.

Firms contemplating using GenAI tools and technologies may want to consider the following:

- *General*:
  - ☐ Developing supervisory processes to develop and use GenAI at an enterprise level.
  - ☐ Approaches to identify and mitigate associated risks, including, but not limited to, accuracy (*e.g.,* hallucinations) and bias:
    - Hallucinations refer to instances where the model generates information that is inaccurate or misleading, yet is presented as factual information.
      - Misrepresentation or incorrect interpretation of rules, regulations or policies or inaccurate client or market data can impact decision making.
    - Bias refers to situations where a model's outputs are skewed or incorrect due to model design decisions or data that is limited or inaccurate, including outdated training data leading to concept drifts.
      - GenAI outputs and decision making could be influenced by historical data, model design or limited/skewed training data.
  - ☐ Assessing whether the firm's cybersecurity program appropriately contemplates:
    - risks associated with the firm's and its third-party vendors' use of GenAI; and
    - how its technology tools, data provenance and processes identify how threat actors use AI or GenAI against the firm or its customers.
- *Supervision & Governance:*
  - ☐ Implementing formal review and approval processes to assess and evaluate GenAI opportunities and the necessary controls to help manage unique risks, including both business and technology experts.
  - ☐ Establishing a supervision, governance or model risk management framework that establishes clear policies and procedures to develop, implement, use and monitor GenAI, while maintaining comprehensive documentation throughout.
- *Testing:* Robust testing of GenAI to understand the capabilities, limitations and performance of the model. Testing areas to consider include areas such as privacy, integrity, reliability and accuracy.
- *Monitoring:* Ongoing monitoring of prompts, responses and outputs to confirm the GenAI solution continues to perform as expected and results in compliant behavior. This may include storing prompt and output logs for accountability and troubleshooting; tracking which model version was used and when; and validation and human-in-the-loop review of model outputs, including performing regular checks for errors or bias.

## Emerging Trends in GenAI: Agents

AI agents are systems or programs that are capable of autonomously performing and completing tasks on behalf of a user. An AI agent can interact within an environment, plan, make decisions and take action to achieve specific goals without predefined rules or logic programming. These agents can enhance GenAI capabilities by providing users with additional opportunities for task automation and the ability to interact with a wider range of data and systems faster and at a potentially lower cost than more traditional process automation.

While AI agents may offer many potential benefits, there are also notable risks and challenges that could result in adverse impacts to investors, firms or the markets:

- *Autonomy:* AI agents acting autonomously without human validation and approval.
- *Scope and Authority:* Agents may act beyond the user's actual or intended scope and authority.
- *Auditability and Transparency:* Complicated, multi-step agent reasoning tasks can make outcomes difficult to trace or explain, complicating auditability.
- *Data Sensitivity:* Agents operating on sensitive data may unintentionally store, explore, disclose or misuse sensitive or proprietary information.
- *Domain Knowledge:* General-purpose AI agents may lack the necessary domain knowledge to effectively and consistently carry out complex and industry-specific tasks.
- *Rewards and Reinforcement:* Misaligned or poorly designed reward functions could result in the agent optimizing decisions that could negatively impact investors, firms or markets.
- *Unique Risks of GenAI:* Keep in mind that the unique risks of GenAI—bias, hallucinations, privacy—also remain present and applicable for GenAI agents and their outputs.

Firms exploring and developing AI agents may wish to consider whether the autonomous nature of AI agents presents the firm with novel regulatory, supervisory or operational considerations. The rapidly evolving landscape and capabilities of AI agents may call for supervisory processes that are specific to the type and scope of the AI agent being implemented. Considerations may include:

- how to monitor agent system access and data handling;
- where to have "human in the loop" agent oversight protocols or practices;
- how to track agent actions and decisions; or
- how to establish guardrails or control mechanisms to limit or restrict agent behaviors, actions or decisions.

FINRA will continue to engage with firms on GenAI and emerging trends as the technology progresses.

## Additional Resources

- FINRA
  - FINRA Blog Post: Advancing FINRA's Mission With AI (October 2025)
  - How FINRA Member Firms Use GenAI (July 2025)
  - FINRA Investor Insight: Protecting Your Investment Accounts from GenAI Fraud (Jan. 15, 2025)
  - Frequently Asked Questions About Advertising Regulation, Questions B.4 and D.8 (May 10, 2024)
  - FINRA Podcast: An Evolving Landscape: Generative AI and Large Language Models in the Financial Industry (March 5, 2024)
  - *Regulatory Notice* 24-09 (FINRA Reminds Members of Regulatory Obligations When Using Generative Artificial Intelligence and Large Language Models)
  - *Regulatory Notice* 24-10 (FINRA Reminds Members of its Policy Prohibiting Members from Recording FINRA Calls and Meetings)
  - *Regulatory Notice* 21-29 (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors)
  - FINRA Report – Artificial Intelligence (AI) in the Securities Industry (June 10, 2020)
- FINRA, SEC and NASAA
  - FINRA, SEC, NASAA Investor Insight: Artificial Intelligence (AI) and Investment Fraud (Jan. 25, 2024)
- National Institute of Standards and Technology (NIST)
  - Artificial Intelligence Risk Management Framework (AI RMF 1.0) (January 2023)

# Firm Operations

## THIRD-PARTY RISK LANDSCAPE

### Regulatory Obligations

FINRA expects firms to establish and maintain a reasonably designed supervisory system, including establishing, maintaining and enforcing written supervisory procedures for outsourcing activities to ensure compliance with applicable securities laws and regulations and FINRA rules.

FINRA encourages firms that use—or are contemplating using—third-party vendors to assess whether their supervisory procedures and controls for outsourced activities or functions are sufficient to maintain compliance with applicable rules—for example, FINRA Rule 1220 (Registration Categories), FINRA Rule 3110 (Supervision) and FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information), and SEC Regulation S-P.

Additionally, FINRA has observed an increase in the reporting of cyberattacks and outages at firms' third-party vendors. Given the financial industry's reliance on third-party vendors to support key systems and covered functions,[20] an attempted cyberattack or an outage at a third-party provider could potentially impact a large number of member firms. FINRA continues to monitor third-party provider risks in the interests of member firms.

#### FINRA's Firm Outreach

FINRA's Risk Monitoring program engages with firms on an ongoing basis to understand how firms use and supervise third-party vendors.

- In January 2025, FINRA issued a request for firms to update information related to their engagements with third-party vendors, particularly those they use for mission-critical systems and functions. This information supplemented FINRA's understanding of the potential impact and effect a third-party vendor cybersecurity event might have on our firms and the securities markets.
- FINRA has used the information gathered to quickly and proactively alert firms of cybersecurity and other vendor-related events that may impact their firm.

Firms can contact their Risk Monitoring Analyst to report any changes to third-party vendors that support their key systems or any cybersecurity events at these vendors.

- New in 2025, as a key component of the FINRA Forward initiatives, FINRA has launched FINRA Cyber & Operational REsilience (CORE). CORE identifies, assesses and shares cyber and technology risk intelligence directly with potentially impacted firms, delivering actionable insights and mitigation tactics. Additionally, CORE enhances visibility of risks and threats across the broker-dealer landscape, enabling early detection of vendor-related threats, systemic technology failures and emerging cyber-attack patterns, aiding in investor protection and market integrity efforts.

## Effective Practices

- Conduct initial and ongoing due diligence on third-party vendors supporting **mission-critical** systems (*e.g.*, information technology and cybersecurity, AML monitoring), **including:**
  - **assessing** the third-party vendor's use of GenAI[21] in their products or services;
  - ensuring contracts with third-party vendors comply with regulatory obligations (*e.g.*, adding language that prohibits firm or customer sensitive information from being ingested into a third-party vendor's open-source GenAI tool); and
  - validating data protection controls in third-party vendor contracts.
- Maintain an inventory of all third-party vendor-provided services, hardware, systems and software components—including the version—used by the firm.
- **Maintain an inventory of firm data types accessed or stored by the firm's vendors.**
- Assess the potential impact of a cybersecurity incident or technology outage at a third-party vendor.
- **Monitor third-party vendor services for vulnerabilities or data breaches.**
- Establish adequate third-party vendor risk management policies and supervisory controls, including risk assessments and contingency plans.
- Review and adjust third-party vendor tool default features and settings to meet business needs and applicable regulatory obligations.
- Involve third-party vendors in firm Incident Response Plan testing.
- **Incorporate** procedures to return or **destroy** firm data at the termination **or conclusion** of a vendor contract.
- Ensure vendor access to systems, data and corporate infrastructure is revoked when the relationship ends.
- Assess the risk of any fourth-party vendors handling firm data.

## Additional Resources

- FINRA
  - **FINRA Unscripted Podcast: Vendor Vigilance: Navigating Third-Party Risk (May 6, 2025)**
  - **Blog Post: Vendors, Intelligence Sharing and FINRA's Mission**
  - FINRA Cybersecurity Advisory: Increasing Cybersecurity Risks at Third-Party Providers
  - *Regulatory Notice* 21-29 (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors)
  - *Notice to Members* 05-48 (Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers)
  - **Cyber & Operational REsilience (CORE) Info sheet**
  - **Cyber Workshops & Tabletop Exercises Info sheet**

## Technology Management

Effective technology management factors significantly into regulatory compliance. When technology systems member firms rely on experience outages, operate sub-optimally or lack appropriate controls, the consequences can impact a firm's ability to meet its regulatory obligations. Below are some effective practices related to technology management FINRA has observed at member firms.

- *Governance:* Establishing a comprehensive technology governance framework with clear accountability, oversight structures and documented processes to systematically identify, assess, mitigate and monitor technology risks across the enterprise. Documenting in firm WSPs, including change, incident and problem management.
- *Risk Assessments:* Regularly assessing firm's technology risk profile based on changes in the firm's size, business model and technology stack. Regularly updating the firm's Information Technology Governance program based on those assessments.
- *Artificial Intelligence (AI)/Large Language Models (LLMs):* Establishing a supervision, governance or model risk management framework that establishes clear policies and procedures for AI/LLM development, implementation, use and monitoring, while maintaining comprehensive documentation throughout. Ensuring comprehensive data management in AI/LLM systems address data quality, integrity, retention and data security.[22]
- *Identity Access Management:* Implementing identity access management controls enforcing least-privilege principles, requiring multi-factor authentication, and maintaining comprehensive access reviews to prevent unauthorized system access and protect sensitive data for human and non-human accounts.
- *Data Backups:* Completing regular backups of critical data and systems, and ensuring the backup copies are encrypted and stored off-network. Regularly testing the recovery of data from backups to confirm information can be restored.
- *Branch Office Procedures:* Limiting the use of branch-managed servers for email or other applications (*e.g.*, customer relationship management, reporting). If branch-managed servers or applications are permitted, ensuring devices and applications are inventoried.
- *Configuration Management:* Confirming desktops, laptops, applications and servers are inventoried and configured to the standards needed for the firm to conduct business.
- *Digital Transformation and the Adoption of Cloud:* Planning and designing processes used when adopting cloud-based systems or technology to confirm adequate preparation.
- *Log Management:* Capturing and retaining log data from a broad set of sources according to factors like compliance requirements, business needs and type of data.
- *IT Resiliency:* Implementing and testing firm controls, and, where relevant, vendor controls, to maintain acceptable service levels during disruption of critical IT systems or services.

# OUTSIDE BUSINESS ACTIVITIES AND PRIVATE SECURITIES TRANSACTIONS

## Regulatory Obligations

FINRA Rules 3270 (Outside Business Activities of Registered Persons) and 3280 (Private Securities Transactions of an Associated Person) require registered persons 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 prohibit, 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.

### FINRA Requested Comment on Proposed New FINRA Rule 3290 to Streamline the Obligations Under FINRA Rules 3270 and 3280

- Earlier in 2025, FINRA released *Regulatory Notice 25-05* (FINRA Requests Comment on a Proposal to Reduce Unnecessary Burdens and Simplify Requirements Regarding Associated Persons' Outside Activities).
- The proposal is intended to enhance efficiency without compromising protections for investors and members relating to outside activities.
- FINRA received more than 200 comments, which helped inform further refinements of the proposal.
- In July, the Board of Governors approved a revised proposal for filing with the SEC.
- As of the date of this publication, FINRA staff are preparing the filing for submission to the SEC.
- The current requirements under Rules 3270 and 3280 continue to apply until any changes are approved by the SEC and become effective.

## Findings

- *Incorrect Interpretation of Selling Compensation for Potential PSTs:* Interpreting "selling compensation" too narrowly (by focusing on only direct compensation, such as commissions, rather than evaluating all direct and indirect financial benefits from PSTs, such as receipt of securities); and, as a result, erroneously determining that certain activities were not PSTs for compensation.
- *Inadequate Approval Process for Potential PSTs:* Approving participation in proposed PSTs for compensation without adequately considering how the individual's participation in the proposed PSTs would be supervised.
- *No Documentation:*
  - Not supervising a person's participation in PSTs for compensation or recording such transactions on the firm's books and records.

- Not retaining the documentation necessary to demonstrate the firm's compliance with the supervisory obligations for PSTs involving compensation.
- Not recording transactions for compensation on the firm's books and records because certain PSTs were not consistent with the firm's electronic systems (such as where securities transactions conducted by an associated person 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 provide prior written notice to their firms of OBAs or, for associated persons, of 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 the firm's limitations placed on OBAs or PSTs, such as prohibiting registered persons from soliciting firm clients to participate in an OBA or PST.

## Effective Practices

- *Questionnaires:* Requiring registered persons 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, which include questions concerning:
  - 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, payments, or direct and indirect financial benefits they receive from any entities other than the firm, including affiliates.
- *Due Diligence:* Conducting due diligence to learn about all OBAs and PSTs at the time of a registered person's initial disclosure to the firm and periodically thereafter, including interviewing the registered person 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 investment advisers or fund companies in order to identify potential PSTs.
- *Monitoring:* Monitoring significant changes in, or other red flags relating to, registered persons' 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;
- financial records (including bank statements and tax returns);
- branch office activities; and
- gifts and gratuities logs.

- *WSPs:* Clearly identifying types of activities or investments that would constitute an OBA or PST, as well as defining selling compensation and in some cases providing FAQs to remind employees of scenarios that they might not otherwise consider, which could 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 public 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.

### Additional Resources

- FINRA
  - *Notice to Members* 96-33 (NASD Clarifies Rules Governing RR/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

Several SEC and FINRA rules address firms' obligations with regards to maintaining and preserving required books and records—for example, SEA Rules 17a-3 and 17a-4 and FINRA Rules 2210(b)(4) (Recordkeeping), 3110(b)(1) (Written Procedures), 3110.09 (Retention of Correspondence and Internal Communications) and 4511 (General Requirements).

SEA Rules 17a-3 and 17a-4 specify minimum requirements with respect to the records that broker-dealers must make, how long those records must be kept and the formats in which they may be kept. FINRA Rule 4511(a) (General Requirements) also requires firms to make and preserve books and records as provided under the FINRA rules, the SEA and applicable SEA rules.

Among other records, firms are required to maintain and preserve specified financial records and records of business-related communications. For example, SEA Rules 17a-3(a)(11) and 17a-4(b)(5) address the recordkeeping requirements related to monthly trial balances,

computations of aggregate indebtedness and net capital computations. In addition, SEA Rule 17a-4(b)(4) and FINRA Rules 3110.09 (Retention of Correspondence and Internal Communications) and 2210(b)(4) (Recordkeeping) address the recordkeeping requirements pertaining to business-related communications, including those received and sent via email, instant message, text message, chat message and interactive blog.

FINRA Rule 3110(b)(1) (Written Procedures) also requires firms to 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 regulations, and with applicable FINRA rules. This requirement includes procedures relating to firms' recordkeeping obligations.

SEA Rule 17a-4(f) also sets forth format requirements for broker-dealers that wish to maintain and preserve required books and records on an electronic recordkeeping system. Specifically, such records must be preserved consistent with the non-rewritable, non-erasable (*i.e.*, WORM) requirement, or consistent with the audit-trail requirement, as described under SEA Rule 17a-4(f).

## Findings

- ***Discrepancies in Financial and Operational Combined Uniform Single (FOCUS) Reports, Net Capital and Reserve Formula Reporting:*** **Inaccurate books and records (*e.g.,* general ledger, trial balance) resulting in discrepancies with firms' net capital and the reserve formula computations. Firms have reported inaccurate FOCUS Reports due to inaccurate calculations of the firm's net capital, aggregate indebtedness, revenue, liabilities and reserve formula computation (where applicable), resulting in violations of SEA Rules 17a-3, 17a-4 and 17a-5, and FINRA Rule 4511.**
- *Failure to Maintain Certain Electronic Communications:* Not retaining, archiving and reviewing non-email electronic communications conducted through firm-approved channels.
- ***Failure to Maintain Electronic Correspondence of Part-Time CCOs or FINOPs:*** **Not capturing, reviewing and archiving electronic correspondence of associated persons—including part-time Chief Compliance Officers (CCOs) and Financial and Operations Principals (FINOPs)—conducting firm business via third-party vendor email addresses.**
- *Failure to Maintain Converted Records:* Not maintaining policies and procedures and related controls to protect the integrity of records for the duration of the applicable retention period, and to confirm physical books and records converted to electronic records were accurate, complete and readable.
- *Inadequate Due Diligence of Third-Party Vendors:* Not performing adequate due diligence to verify third-party vendors' ability to comply with recordkeeping requirements; or not confirming that service contracts and agreements comply with applicable recordkeeping requirements, including records stored by third-party vendors.
- *Inadequate Supervision:*
  - Not reviewing electronic communications for indications of associated persons' potential use of off-channel communications for business-related communications.[23]

- Not establishing procedures and controls to retain and review written, business-related electronic communications made through non-firm-approved email accounts and other communication tools.
- Not retaining and reviewing business-related text messages.
- Not properly supervising third-party vendors that support firms' monitoring of their associated persons' electronic communications, resulting in firms not capturing, retaining or supervising communications.

- *Inadequate WSPs:* Relying on policies and procedures that were overly general and did not adequately specify:
  - permitted and prohibited business communication platforms;
  - methods to determine if associated persons are engaging in business communications on unapproved platforms; and
  - corrective action for associated persons if they violate firm policy and engage in business communication using unapproved platforms.
- *Contacting Firm Customers Through Off-Channel Platforms:* Associated persons using personal email accounts or other off-channel platforms to communicate with customers regarding firm business without the firm's knowledge.
- *Inadequate Reviews:* Reviewing electronic communications without selecting adequate samples or using targeted key word searches; and failing to review electronic communications in non-English languages in which the member conducts business.

## Effective Practices

- *Testing and Verification:* Testing third-party recordkeeping vendors' capabilities to fulfill regulatory obligations by, for example, simulating a regulator's examinations by requesting records to confirm compliance with the recordkeeping requirements.
- *Providing Appropriate Access to Books and Records:* If the firm uses a part-time FINOP, contracted CCO or part-time employee or contractor for other roles, ensuring there is a process in place to provide appropriate access to the firm's books and records to allow for the individuals to fulfill their regulatory obligations.
- *Supervisory Procedures:*
  - Monitoring for indications that associated persons are using off-channel communications (*e.g.*, a decrease or absence of activity on certain previously used firm-approved communication channels or tools).
  - Frequently revising key words used to surveil for associated persons' potential use of off-channel communications, and tailoring keyword searches to the business models.

### Additional Resources

- FINRA
  - Books and Records Key Topics Page
  - Books and Records Requirements Checklist
  - Exchange Act Rule 17a-4 Amendments: Chart of Significant Changes
  - *Regulatory Notice 18-31* (SEC Staff Issues Guidance on Third-Party Recordkeeping Services)
  - Frequently Asked Questions about the 2001 Amendments to Broker-Dealer Books and Records Rules Under the Securities Exchange Act of 1934
  - **Regulatory Notifications – Failure to Make and Keep Current Books and Records (Updated April 27, 2024)**

## SENIOR INVESTORS AND TRUSTED CONTACT PERSONS

### Regulatory Obligations

Several FINRA rules address firms' regulatory obligations regarding senior investor protection—including FINRA Rules 4512(a)(1)(F) (Customer Account Information), 3241 (Registered Person Being Named a Customer's Beneficiary or Holding a Position of Trust for a Customer) and 2165 (Financial Exploitation of Specified Adults).

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.

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.

FINRA Rule 2165 (Financial Exploitation of Specified Adults) permits firms to place temporary holds on a disbursement of funds or securities and securities transactions when firms reasonably believe that financial exploitation has occurred, is occurring, has been attempted or will be attempted, and requires firms to notify the TCP, if available, when placing temporary holds.

FINRA's examination and enforcement programs also focus on a broad range of topics relating to the protection of senior investors, and we have brought disciplinary actions against firms that have mistreated seniors. Relevant findings are captured in other sections of this Report.

## 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 the 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 customer opens a new non-institutional account).
- *No Documented Training:* Relying on FINRA Rule 2165 but not developing and documenting training policies or programs reasonably designed to ensure associated persons comply with the requirements of the rule.
- *No Documented Internal Review:* Relying on FINRA Rule 2165 but not retaining records that document the firm's internal review underlying the decision to place a temporary hold on a disbursement or transaction.
- *Attempted Circumvention of FINRA Rule 3241:* Registered persons attempting to circumvent the rule's requirements by having customers name the registered person's spouse or other family members as beneficiaries for customers' accounts.

### FINRA Resources and Workshops Related to Senior Investor Protection

In honor of World Elder Abuse Awareness Day 2025, FINRA, NASAA and the SEC published Senior Investor Protection Resources For Broker-Dealers, which includes:

- key websites;
- relevant *Regulatory Notices*, advisories and guidance;
- training resources;
- helplines;
- resources for reporting suspected financial exploitation and criminal activity; and
- educational resources broker-dealers may share with senior investors.

FINRA also offers Senior Investor Financial Exploitation Case Study Workshops, which focus on how to identify, aid and manage threats targeting senior investors. On-demand recordings of prior workshops are available on FINRA's website; visit the Compliance Workshops page for an up-to-date schedule of upcoming offerings.

For additional guidance related to recognizing and preventing senior investor fraud, please see FINRA's Senior Investors Key Topics Page and these *Investor Insights* articles:

- Protect Your Money—Protecting Older Investors From Financial Exploitation
- Avoid Fraud—Relationship Investment Scams: What They Are and Tips to Avoid Them

## Effective Practices

- *Customer Outreach:* Engaging in communication campaigns on fraud awareness, hosting educational webinars and providing customers with other resources to educate them on the latest scams **(*e.g.*, FINRA Investor Insights articles, FBI's Annual IC3 Report).**
- *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 **to increase likelihood of a designation, such as requiring a "yes" or "no" response to the TCP question in account opening forms or asking, "Who is your trusted contact?" rather than, "Would you like to name a trusted contact?"**
  - 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.
  - Providing guidance to registered representatives regarding contacting TCPs when the firm places a temporary hold.
- *Supervisory Procedures:* When establishing procedures for FINRA Rule 2165 related to placing temporary holds, contemplate how the firm will ensure supervisory procedures and WSPs related to the identification, escalation and reporting of matters involving the financial exploitation of specified adults will be handled.
- *Escalation Process:* Implementing and training registered representatives to use a comprehensive process to escalate issues relating to seniors, including but not limited to concerns about financial exploitation, diminished capacity or cognitive decline.
- *Senior Investor Specialists:* Establishing specialized groups or appointing individuals to handle situations involving elder abuse or diminished capacity; contacting customers' TCPs—as well as Adult Protective Services, regulators and law enforcement, when necessary—and guiding the development of practices focused on senior customers.
- ***Expanding and Centralizing Firm Resources:* Developing internal dashboards to assist associated persons in working with senior investors (*e.g.*, information on trusted contacts and powers of attorney); preparing "playbooks" for associated persons who suspect financial exploitation to assist in determining whether to escalate an issue.**
- *Training:*
  - Conducting training, for both front office and back office staff, on common financial and investment scams and the warning signs of potential: (1) fraud or exploitation perpetrated on the customer; or (2) diminished capacity.
  - Conducting training, for both front office and back office staff, on effective communication with potential victims of elder financial exploitation.

## Additional Resources

- FINRA
  - Senior Investors Key Topics Page
  - **Senior Investor Protection Resources for Broker-Dealers**
  - Threat Intelligence Product: Protecting Vulnerable Adult and Senior Investors
  - **2025 FINRA Annual Conference: Mitigating Impacts and Scams Targeting Senior Customers**
  - 2024 FINRA Annual Conference: Advances in Senior Investor Protection
  - **10 Facts About the FINRA Securities Helpline for Seniors**
  - **Three Resources for Senior Investors**
  - *Regulatory Notices*
    - ***Regulatory Notice 25-07* (FINRA Requests Comment on Modernizing FINRA Rules, Guidance, and Processes for the Organization and Operation of Member Workplaces), Section G. Fraud Protection**
    - *Regulatory Notice 22-31* (FINRA Shares Practices for Obtaining Customers' Trusted Contacts)
    - *Regulatory Notice 22-05* (FINRA Adopts Amendments to FINRA Rule 2165)
    - *Regulatory Notice 20-38* (FINRA Adopts Rule to Limit a Registered Person From Being Named a Customer's Beneficiary or Holding a Position of Trust for or on Behalf of a Customer)
    - *Regulatory Notice 20-30* (Fraudsters Using Registered Representatives Names to Establish Imposter Websites)
    - *Regulatory Notice 19-18* (FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations)
  - FINRA Unscripted Podcasts
    - **Protecting Investors: FINRA Securities Helpline for Seniors' 10th Anniversary (April 1, 2025)**
    - Fighting Financial Exploitation: FINRA's Vulnerable Adults and Seniors Team (April 30, 2024)
    - **Preventing Financial Exploitation: Steps for Safeguarding Senior Investors (June 27, 2023)**
    - The Essential Senior Investor Protection Tools: FINRA Rules 2165 and 4512 (May 3, 2022)
- FINRA, NASAA and SEC
  - NASAA/SEC/FINRA Training: Addressing and Reporting Financial Exploitation of Senior and Vulnerable Adult Investors (June 2023)
- **FBI**
  - **FBI Elder Fraud Report 2024**
- FinCEN
  - Elder Financial Exploitation: Threat Pattern & Trend Information, June 2022 to June 2023 (April 2024)
- Consumer Financial Protection Bureau (CFPB)
  - Protecting older adults from fraud and financial exploitation

# Member Firms' Nexus to Crypto

## Regulatory Obligations

Crypto assets—also known as digital assets—are assets that are generated, issued or transferred using a blockchain or similar distributed ledger technology network. While many kinds of market participants engage in crypto asset activities, FINRA has jurisdiction only over its member firms and their associated persons. Federal securities laws and FINRA rules generally apply to member firm activities involving crypto assets that are securities, including those that are offered and sold as an investment contract (which is a type of security). In addition, certain FINRA rules apply to the activities of firms and their associated persons irrespective of whether the activity involves a security.

**FINRA is actively monitoring and responding to market, legislative and policy developments in this rapidly evolving area and encourages member firms to do the same. Examples include the following:**

- **The enactment of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act)—which establishes a regulatory framework for the issuance stablecoins—on July 18, 2025**
- **SEC Division of Corporation Finance: Crypto Asset Exchange-Traded Products (July 1, 2025)**
- **SEC Division of Trading and Markets: Withdrawal of Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities (May 15, 2025)**
- **SEC Division of Trading and Markets: Frequently Asked Questions Relating to Crypto Asset Activities and Distributed Ledger Technology (May 15, 2025)**
- **SEC Division of Corporation Finance: Offerings and Registrations of Securities in the Crypto Asset Markets (April 10, 2025)**
- **SEC Division of Corporation Finance: Statement on Stablecoins (April 4, 2025)**
- **SEC Division of Corporation Finance: Statement on Certain Proof-of-Work Mining Activities (March 20, 2025)**
- **SEC Division of Corporation Finance: Staff Statement on Meme Coins (Feb. 27, 2025)**

## Findings

- *FINRA Rule 2210 (Communications with the Public):*
  - Not including appropriate disclosures in communications with the public about relevant risks.[24]
  - Disseminating promotional materials in connection with securities offerings involving crypto assets that contained false and misleading statements or material omissions.

- Comparing the crypto asset to other assets (*e.g.,* stock investments or cash) without providing a sound basis to compare the varying features and risks of crypto assets.
- Making misleading statements about the extent to which certain crypto assets were protected by the Securities Investor Protection Corporation (SIPC) under the Securities Investor Protection Act (SIPA).
- **Social media communications posted by influencers on a firm's behalf that were not fair and balanced or made claims that were promissory or misleading.**
- **Not disclosing that the crypto assets were not offered through the member firm (*e.g.*, promoting crypto assets offered by an affiliate without disclosing that they were not offered by the member firm).**

- *FINRA Rule 3110 (Supervision):* Not conducting appropriate due diligence on the crypto asset **securities, crypto asset-related** private placements **of securities, and crypto asset-related securities products that the firm recommends** to customers.
- ***FINRA Rules 3270 (Outside Business Activities of Registered Persons) and 3280 (Private Securities Transactions of an Associated Person):* Failures related to the disclosure of crypto asset outside business activities and the approval and supervision of private securities transactions for selling compensation (*e.g.*, soliciting investments in, and receiving selling compensation for, securities issued by a company claiming to operate crypto asset mining and investment programs without prior written notice to or approval from the associated person's employing firm).**
- ***FINRA Rule 3310 (Anti-Money Laundering (AML) Compliance Program):* Not establishing and implementing AML programs reasonably designed to detect and cause the reporting of suspicious crypto asset transactions occurring by, at or through the broker-dealer.**
- ***FINRA Rule 11870 (Customer Account Transfer Contracts):* Improperly rejecting customer requests to transfer assets within their brokerage accounts via the ACATS process if the customer also maintained a separate account that had a crypto asset balance at the firm's affiliate.**
- ***FINRA Rule 2010 (Standards of Commercial Honor and Principles of Trade):* Negligently causing the dissemination of promotional materials that the member firm or associated person should have known contained material misstatements and omitting material facts related to the member firm's crypto asset business.**

## Effective Practices

- *Due Diligence on Unregistered Offerings:*[25] Before crypto assets that are securities or that are offered and sold as securities are recommended to customers through an unregistered offering, understanding:
  - the exemption from registration on which the unregistered offering will rely;
  - whether the offering is a contingent offering, and, if it is, the relevant contingencies and how the funds or assets will be returned in the event of a contingent offering not meeting the minimum contingency;

- **description of the business and** how the raised proceeds will be used;
- **risk factors and conflicts of interest disclosed in the prospectus, offering documents or other promotional materials; and**
- the specific mechanics associated with the crypto asset that is a security or that is offered or sold as a security, including:
  - **the identities and background of the initial development team (*e.g.,* to review for potential conflicts);**
  - **the total supply of the underlying crypto assets, whether there is a cap on supply and what the minting and burning schedule is, as well as any material events impacting the supply of the crypto assets such as halving events and protocol modifications;**
  - **any markets associated with the crypto asset(s);**
  - any smart contract features or functionalities **(including related cybersecurity risks);**
  - how and when the security will be delivered to customers; and
  - how the security will be custodied by or for customers.

- *On-Chain Reviews:* Conducting risk-based on-chain fraud and anti-money laundering reviews when the firm or its associated persons are accepting, trading or transferring crypto assets, and establishing procedures that address when and how these on-chain reviews are performed and documented.

- *Informing Customers:* Ensuring customers **are informed about**:
  - the differences between their brokerage account and any linked or affiliated crypto account; and
  - differences in:
    - protections **of assets** in the accounts via SIPC under SIPA;
    - regulatory oversight;
    - firm supervision; and
    - avenues of communications for customers' concerns, questions or complaints.

### FINRA continues to encourage firms to notify FINRA about new and planned activities related to crypto assets:

- FINRA has issued guidance encouraging firms to notify FINRA about new and planned activities related to digital assets:
  - *Regulatory Notice 21-25* (FINRA Continues to Encourage Firms to Notify FINRA if They Engage in Activities Related to Digital Assets)
  - *Regulatory Notice 20-23* (FINRA Encourages Firms to Notify FINRA if They Engage in Activities Related to Digital Assets)
- Additionally, firms can contact their Risk Monitoring Analyst if they have questions about their engagement, or potential engagement, with crypto assets.

## Additional Resources

- FINRA
  - The Communications with the Public topic
  - Crypto Assets Key Topics Page, including:
    - FINRA Provides Update on Member Firms' Crypto Asset Activities (Aug. 13, 2024)
    - FINRA Provides Update on Targeted Exam: Crypto Asset Communications (Jan. 23, 2024)
  - FINRA Unscripted Podcasts
    - An Update on FINRA's Crypto Asset Work and the Crypto Hub (July 23, 2024)
    - Compliance and Communication: An Update on FINRA's Crypto Asset Targeted Exam (Jan. 23, 2024)
- SEC
  - **Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act) (July 18, 2025)**
  - **Division of Corporation Finance: Crypto Asset Exchange-Traded Products (July 1, 2025)**
  - **Division of Trading and Markets: Withdrawal of Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities (May 15, 2025)**
  - **Division of Trading and Markets: Frequently Asked Questions Relating to Crypto Asset Activities and Distributed Ledger Technology (May 15, 2025)**
  - **Division of Corporation Finance: Offerings and Registrations of Securities in the Crypto Asset Markets (April 10, 2025)**
  - **SEC Division of Corporation Finance: Statement on Stablecoins (April 4, 2025)**
  - **SEC Division of Corporation Finance: Statement on Certain Proof-of-Work Mining Activities (March 20, 2025)**
  - **SEC Division of Corporation Finance: Staff Statement on Meme Coins (Feb. 27, 2025)**
  - **SEC Staff Accounting Bulletin No. 122 (Rescission of SAB 121) (Jan. 30, 2025)**
  - Custody of Digital Asset Securities by Special Purpose Broker-Dealers (Dec. 23, 2020)
  - ATS Role in the Settlement of Digital Asset Security Trades (Sept. 25, 2020)

# Communications and Sales

## COMMUNICATIONS WITH THE PUBLIC

### Regulatory Obligations

FINRA's communication rules—including FINRA Rules 2210 (Communications with the Public) and 2220 (Options Communications)—are based on the principles of ensuring that member communications are fair and balanced, and that investors do not receive misleading information. 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.

FINRA Rule 2210 defines three categories of written communications—correspondence, retail communications or institutional communications—and sets principles-based content standards that are designed to apply to evolving communications technology and practices. **FINRA's Advertising Regulation Department reviews communications firms submit either voluntarily or as required by FINRA Rule 2210.** New firms are required to file all widely disseminated retail communications with FINRA's Advertising Regulation Department during their first year of membership, and all firms are subject to filing requirements for specified retail communications depending on their content.

FINRA Rule 2220 (Options Communications) governs firms' communications with the public concerning options.

### Findings

- *Inadequate Supervision of Firms' Social Media Influencers **and Failure to Retain Records***:
  - Not establishing, maintaining and enforcing a system, including WSPs, reasonably designed to supervise communications disseminated on the firm's behalf by influencers.
  - Not reviewing **and approving** influencers' **static content on behalf of the firm** prior to **the influencer** posting on social media platforms.
  - **Not reviewing or supervising influencer communications on the firm's behalf posted in online interactive electronic forums in the same manner as required for supervising and reviewing firm correspondence.**
  - **Not retaining retail communications influencers post on the firm's behalf.**
- *False, Misleading, Inaccurate **or Unbalanced** Information in Mobile Apps:*
  - **Failing to disclose or inaccurately disclosing the risk of loss associated with certain options transactions.**
  - Distributing false or misleading promotions through social media and "push" notifications or "nudges" on mobile apps that made promissory claims or omitted material information.
  - Failing to fully explain the products or services being offered.

- Failing to clearly and prominently disclose risks, where required by a specific rule or needed to balance promotional content, particularly claims associated with complex products and strategies such as options trading, the use of margin and crypto assets.

- *Inadequate Reviews:* Reviewing electronic communications without selecting adequate samples or using targeted key word searches; and failure to review electronic communications in non-English languages in which the member conducts business.

## Effective Practices

- *Procedures for Mobile Apps:* Maintaining and implementing supervisory procedures for mobile apps that, for example, verify the accuracy of information and data displayed to customers.

- *Reasonably Designed Procedures for Digital Communications:* Establishing, maintaining and enforcing reasonably designed procedures for supervision of digital communication channels, including:
  - *Monitoring of New Tools and Features:* Monitoring new communication channels, apps and features available to associated persons and customers;
  - *Defining and Enforcing Prohibited Activity:* Clearly defining permissible and prohibited digital communication channels, tools and features, and blocking those prohibited channels, tools and features that prevent firms from complying with their **supervision and** recordkeeping requirements;
  - *Supervision:* Implementing supervisory review procedures tailored to each digital channel, tool or 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; and
  - *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 before resuming use.
  - *GenAI:*
    - When using GenAI to generate or otherwise assist in creating communications to customers, ensuring that these communications comply with applicable federal securities laws and regulations and FINRA rules.
    - When using GenAI to create or otherwise assist in creating chatbot communications that are used with investors, ensuring the appropriate supervision **and retention** of those communications, and retention of those chat sessions, in accordance with applicable **securities laws and regulations** and FINRA rules.
    - Ensuring that retail communications that mention AI tools or AI services (*e.g.*, portfolio construction or products that rely on AI management) accurately describe how these offerings incorporate AI technology and balance the discussion of benefits with appropriate discussion of risks.[26]

- *Communications Promoting Securities Lending Programs:* Ensuring that communications that promote or recommend income sharing programs to retail investors (*e.g.,* fully paid securities lending programs) accurately and clearly disclose the terms and conditions of the program, including any fees customers would receive.

### Additional Resources

- FINRA
  - Advertising Regulation
  - Social Media Key Topics Page
  - **Frequently Asked Questions about Advertising Regulation, Supervising Chatbot Communications and AI Created Communications**

## REG BI AND FORM CRS

### 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 **when making a recommendation**. The standard of conduct established by Reg BI cannot be satisfied through disclosure alone.

Separately, whether they make recommendations or not, firms that offer services to retail investors must file and provide retail investors with Form CRS, a brief relationship summary in a prescribed format that discloses important information about the firm in plain language (*e.g.*, investment services provided, fees, conflicts of interest, legal and disciplinary history of the firms and associated persons).

### Findings

*Reg BI*

- *Failure to Comply With Care Obligation:*
  - Failing to conduct a reasonable investigation of offerings prior to recommending them to retail customers (*e.g.,* unable to reasonably evidence due diligence efforts regarding the issuer; relying solely on the firm's past experience with and knowledge of an issuer based on previously completed offerings; or relying solely on information from the issuer or its affiliate).[27]
  - Making recommendations of securities or investment strategies involving securities (including account recommendations) without a reasonable basis to believe that they were in the best interest of a particular retail customer, including recommendations of complex or risky products that do not align with the retail customer's investment profile.

- Recommending a series of transactions that were excessive in light of retail customers' investment profiles and factors such as high cost-to-equity ratios and high turnover ratios.
- Recommending that customers replace or switch existing products **or accounts** (*e.g.*, variable annuities, mutual funds, 529 plan accounts) without understanding or considering associated risks and costs, including as applicable, the imposition of penalties (*e.g.*, surrender charges) and new surrender periods, loss of existing benefits, tax consequences and transaction costs.
- Failing to consider or compare relevant costs and fees, such as product or account-level fees, when recommending a product or when determining whether to recommend **that a customer purchase a security** in **either the** customer's brokerage or advisory account, or to recommend transfers of securities between **a customer's** brokerage and advisory accounts.
- Not maintaining profile information collected from retail customers in accordance with SEA Rule 17a-3(a)(35), thereby undermining the firm's and its associated persons' abilities to demonstrate compliance with the Care Obligation.
- Making recommendations of complex or risky products that result in concentrations exceeding limits specified in a firm's policies, or comprising a sizable portion of a retail customer's liquid net worth or securities holdings in a manner that is inconsistent with the retail customer's risk tolerance or investment objectives.

▸ *Failure to Comply With Conflict of Interest Obligation:*

- Not identifying and disclosing, mitigating or eliminating, as appropriate, conflicts of interest associated with recommendations of securities transactions or investment strategies involving securities.
- Not identifying and mitigating (*i.e.*, modifying practices to reduce) conflicts of interest that create an incentive for an associated person to make securities recommendations that place the interests of the associated person or the firm ahead of the interests of the retail customer.
- Not identifying and disclosing all *material* facts concerning *material* conflicts of interest related to an associated person's incentive to recommend particular securities or account types (*e.g.*, an associated person's financial incentive to recommend the opening of new investment accounts at the firm's affiliate).
- Not identifying and addressing all potential conflicts of interest relevant to a firm's business model, including, but not limited to, material limitations on securities or investment strategies and conflicts associated with these limitations.

▸ *Failure to Comply With Disclosure Obligation:*

- Not providing retail customers with "full and fair" disclosures of all material facts related to the scope and terms of their relationship with these retail 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 roll over qualified accounts);

- material limitations in securities offerings; and
- transaction-based fees that were inconsistent with—and, in some cases, materially higher than—those outlined in Reg BI customer disclosures.

- Associated persons, firms or both, improperly using the terms "advisor" or "adviser" in their titles or firm names, even though they lack the appropriate registration and do not engage in other activities that allow the use of those terms **(*e.g.*, a firm that was formerly registered as both a broker-dealer and an investment adviser retaining the term "advisor" or "adviser" in its firm name after withdrawing its registration as an investment adviser).**

- *Failure to Comply with Compliance Obligation:*
  - Failing to adopt and implement written policies and procedures that are reasonably designed to achieve compliance with Reg BI by, for example, stating the rule requirements but failing to identify how the firm will comply with those requirements (*e.g.,* requiring associated persons to consider costs and reasonably available alternatives when making recommendations, but not specifically addressing or detailing how associated persons should do so).
  - Failing to enforce Reg BI procedures or supervisory processes for compliance, such as outlining documentation requirements, and failing to implement any process to confirm associated persons are complying with the firms' requirements or failing to follow up on red flags (*e.g.*, duplicative rationales documented by the same associated person for different types of customers).
  - Failing to **establish written policies and procedures that address how training on the requirements of Reg BI would be conducted and enforced, leading to failures to** conduct adequate or ongoing training of associated persons.
  - Failing to have policies and procedures reasonably designed to achieve compliance with Reg BI regarding recommendations involving variable annuities (VAs) **or registered index-linked annuities** (RILAs) (*e.g.*, not adequately collecting and retaining key information on variable annuity **or RILA** transactions; and not sufficiently training associated persons and supervisors to determine whether variable annuity or RILA exchanges complied with the standards of Reg BI).[28]
  - Failing to have written policies and procedures reasonably designed or enforced with respect to account recommendations, for example, by:
    - not being reasonably designed to address recommended transfers of products between brokerage and **other private wealth management** accounts or rollover recommendations;
    - not being reasonably designed to achieve compliance with the capacity disclosure requirement, including the titling restriction;
    - not following up on red flags such as identified patterns of account switches by the same associated person;
    - requiring documentation of rationale, but not following up on generic or insufficient rationales;

- **not providing any procedures or guidance regarding the factors to consider when recommending a particular account type, such as the costs associated with such accounts and the services provided (including whether the customer was already receiving such services); or**
- **failing to detail any steps a supervisor should take to determine whether an account type recommendation was in the customer's best interest.**

*Form CRS*

- *Deficient Form CRS Filings:* Firms' Form CRS filings significantly departing from the Form CRS instructions or SEC guidance by:
  - inaccurately or inappropriately representing the firm's or its associated persons' disciplinary histories, such as by including qualifying language to explain disciplinary history **(*e.g.*, "Yes. However, our firm has been in business for many decades and never received any customer complaints.");**
  - omitting **or misstating** material facts (*e.g.*, description of services offered, limitations of the firm's investment services, cost disclosures);
  - failing to describe, or inaccurately describing types of compensation and conflicts **of interests such compensation creates;**
  - incorrectly stating that the firm does not provide recommendations; and
  - changing or excluding language required by Form CRS.
- *Failing to Properly Deliver Form CRS:* Failing to deliver or not creating a record of the date on which the firm provided each Form CRS to each retail investor, including failure to deliver Form CRS before **or at the time** such retail investor opened an account.
  - If the relationship summary is delivered electronically, failing to present it prominently in the electronic medium and make it easily accessible for retail investors (*e.g.*, by solely placing a link to the Form CRS in an email footer below the signature line; by including the Form CRS among other disclosures in a ZIP file attachment without any mention of the Form CRS in the email).
- *Failing to Properly Post Form CRS:* 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).
- *Failing to Adequately Amend Form CRS:* Firms not in compliance with Form CRS in relation to material changes because they:
  - failed to timely file **the amended Form CRS** with an exhibit highlighting the changes in the Central Registration Depository (CRD) (*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 investors (*e.g.*, delivering amended **Form CRS**, with required exhibits, showing revised text or summarizing material changes or communicating the information through another disclosure, **in either case** within 60 days after the updates are required to be made (90 days total from the date when Form CRS became materially inaccurate).

## Effective Practices

*Care Obligation*

- *Costs and Reasonably Available Alternatives:* Including in **written policies and** procedures specific factors related to evaluating costs and reasonably available alternatives to recommended products, including but not limited to:
  - providing clear guidance to associated persons making recommendations on how to evaluate costs and reasonably available alternatives, such as by:
    - advising that reasonably available alternatives be considered before a recommendation has been formulated;
    - using worksheets, in paper or electronic form, to compare costs and reasonably available alternatives;
    - creating notes or documents in a similar format to evaluate recommended transactions and provide information on the retail customer's financial situation, needs and goals (and substantiate why that specific recommendation was in the retail customer's best interest);
    - specifying the relevant factors to consider when evaluating costs (*e.g.*, deferred sales charges) and reasonably available alternatives (*e.g.*, similar investment types or less-complex or less-risky products available at the firm);
    - updating client relationship management (CRM) tools to automatically compare recommended products to reasonably available alternatives; or
    - ensuring that any technology used to generate recommendations is coded to consider costs on both affiliated and non-affiliated investment products offered by the firm;
  - setting forth clear **written policies and procedures** that address **supervisory** reviews and firm-required documentation;
  - sampling recommended transactions to evaluate how costs and reasonably available alternatives were considered; and
  - establishing limitations on complex or higher-risk products, such as by using firm concentration limits or minimum liquid net worth requirements.
- *Heightened Scrutiny of Complex or Risky 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;
  - applying heightened supervision to recommendations of products, or investment strategies involving securities, that are complex or risky, or limiting such recommendations to specific customer types; and
  - **appropriately training associated persons on the features of complex and risky products recommended to retail customers.**

*Conflict of Interest Obligation*

- *Policies and Procedures:* Establishing and implementing policies and procedures to address conflicts of interest by:
  - using 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;

- revising commission schedules for recommendations within product types to flatten the percentage payout rate to employees; and
- broadly prohibiting all sales contests, regardless of whether they are required to be eliminated under Reg BI.

*Disclosure Obligation*

- *Implementing Systems Enhancements for Recording the Date of Delivery of Required Customer Documents:* Maintaining a record for delivering Form CRS and Reg BI-related documents to retail customers in a timely manner by:
  - automating mechanisms to evidence delivery of Form CRS and other relevant disclosures; and
  - memorializing delivery of required disclosures at the earliest triggering event.
- *Providing Clear Disclosure on Account Type Recommendations:* Providing retail customers with clear, accessible materials that allow them to compare the features, benefits and costs of certain account type recommendations (*e.g.*, rollovers).

*Compliance Obligation*

- *Implementing New Surveillance Processes:* **Supervising** associated persons' compliance with Reg BI by:
  - conducting reviews to confirm that their recommendations meet Care Obligation requirements, including system-driven alerts or trend criteria to identify:
    - account type or rollover or transfer recommendations that may be inconsistent with a retail customer's best interest;
    - products that are high risk, high cost, complex or represent a significant conflict of interest;
    - excessive trading; and
    - sale of same product(s) to a high number of retail customers; and
  - **supervising** 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.
- Incorporating Reg BI-specific reviews into the branch exam program, in addition to other ongoing monitoring and surveillance.
- Focusing on areas such as documenting Reg BI compliance and following the firms' Reg BI written policies and procedures (as part of overall Reg BI compliance efforts).

## Additional Resources

- FINRA
  - SEC Regulation Best Interest Key Topics Page
  - **Reg BI and Form CRS Firm Checklist**
  - **2025 FINRA Annual Conference: Strengthening Compliance of Regulation Best Interest and Form CRS**

- 2024 FINRA Annual Conference: The Progression of Regulation Best Interest and Form CRS
- *Regulatory Notice 23-20* (FINRA Highlights Available Guidance and Resources Related to Regulation Best Interest)

▸ SEC

- SECs Regulation Best Interest, A Small Entity Compliance Guide
- Regulation Best Interest, Form CRS and Related Interpretations
- Frequently Asked Questions on Regulation Best Interest
- Frequently Asked Questions on Form CRS
- Staff Bulletin: Standards of Conduct for Broker-Dealers and Investment Advisers Care Obligations (April 30, 2023)
- Observations from Broker-Dealer Examinations Related to Regulation Best Interest (Jan. 30, 2023)
- Staff Bulletin: Standards of Conduct for Broker-Dealers and Investment Advisers Conflicts of Interest (Aug. 3, 2022)
- Staff Bulletin: Standards of Conduct for Broker-Dealers and Investment Advisers Account Recommendations for Retail Investors (March 30, 2022)
- Staff Statement Regarding Form CRS Disclosures (Dec. 17, 2021)
- You may submit a question by email to tradingandmarkets@sec.gov; additionally, you may contact the SEC's Division of Trading and Markets' Office of Interpretation and Guidance at (202) 551-5777

## PRIVATE PLACEMENTS

### Regulatory Obligations

Private placements are unregistered, non-public securities offerings that rely on an available exemption from registration with the SEC under either Section 3 or 4 of the Securities Act.

In *Regulatory Notice 23-08* (FINRA Reminds Members of Their Obligations When Selling Private Placements), FINRA noted the obligations of firms that recommend private placements to conduct a reasonable investigation of those securities under Reg BI for recommendations to retail customers and FINRA Rule 2111 (Suitability) for recommendations to non-retail customers, as well as other obligations that could apply even in the absence of a recommendation, including FINRA Rules 2210 (Communications with the Public), 3110 (Supervision), 3280 (Private Securities Transactions of an Associated Person), 5122 (Private Placements of Securities Issued by Members) and 5123 (Private Placements of Securities).

*Regulatory Notice 23-08* updated and supplemented guidance published under *Regulatory Notice 10-22* (Obligations of Broker-Dealers to Conduct Reasonable Investigations in Regulation D Offerings) and **reminded firms that the** reasonable investigation of **a recommended privately offered** security, at a minimum, **should include an evaluation** of "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."

Additionally, FINRA Rules 5122 and 5123 require firms to timely file with FINRA offering documents and information for the private placements they offer or sell, including retail

communications used by the broker-dealer to promote or recommend an offering, unless a filing exemption is available.

## Findings

- *Inadequate Filings Procedures:* Not maintaining policies and procedures, processes and supervisory programs to comply with filing requirements; resulting in a failure to file or untimely filings (with, in some cases, delays as long as six to 12 months); and relying on **a filing** exemption under FINRA Rule 5123(b) **that is not applicable to the offering (*e.g.*, the exemption for sales to certain institutional accredited investors, which is generally not applicable for sales to individual accredited investors).**
- *Failing to Conduct Reasonable Investigation:* Failing to fulfill reasonable-basis obligations prior to recommending private placements to retail investors, by:
  - failing to conduct an appropriate level of research on the issuer's business, particularly when there is a lack of operating history;
  - relying solely on the firm's past experience and knowledge with an issuer based on previously completed offerings;
  - failing to inquire into, analyze and resolve red flags identified during the reasonable investigation process or in third-party due diligence reports; and
  - failing to conduct a reasonable investigation of the issuer, the individuals involved in its management or other "covered persons" under Reg D.
- *Failure to Evidence Due Diligence:* Failing to maintain records of, or otherwise evidence or reasonably explain, due diligence efforts into issuers' financial condition, operations, representations of past performance and involvement in **litigation or any evaluation of "red flags" or problematic claims and representations identified during due diligence.**
- *Improper Discharge of Reg BI Obligations:* Incorrectly purporting to not make recommendations of private placements, or claiming that the issuer is making the recommendations, despite **evidence that representatives communicated a "call to action" to customers concerning the particular security that is** individually tailored to the customer (and as a result, the **firm or its** representatives did not exercise reasonable diligence, care and skill in making such recommendations); **or not adequately identifying, disclosing and, where appropriate, mitigating conflicts of interest associated with recommendations of private placements.**[29]
- *Failure to Comply With SEC Rules Regarding Contingency Offerings:* Participating in a contingency offering without meeting the requirements of SEA Rules 10b-9 and 15c2-4, in particular when the contingency terms are amended during the offering (*e.g.,* reducing the minimum contingency amount).

### Continuing Trend: Private Placement Offerings of Pre-IPO Funds

- FINRA has observed instances of potentially fraudulent activity in the sale of private placement offerings of pre-IPO funds, such as material misrepresentations and omissions concerning sales compensation in connection with the recommendations.
- FINRA has also observed that firms have failed to conduct reasonable due diligence of recommended pre-IPO funds, such as failing to confirm that the fund had possession of or access to the pre-IPO shares that it purported to hold, or failing to understand the costs associated with acquiring the pre-IPO shares.

## Effective Practices

- *Private Placement Checklist:* Amending due diligence checklists to account for specific types of private placements with unique risk factors or conditions that may impact whether they are in the best interest of retail customers.
- *"Bad Actor" Questionnaires:* Reviewing "Bad Actor" forms or similar questionnaires at both the issuer level (*e.g.*, Directors' and Officers' Questionnaires) and placement agent level (*e.g.*, registered representative questionnaires) to support compliance with Rules 506(d) and 506(e) of Regulation D.
- *Independent Review:* Conducting and documenting reviews of material aspects of the offering by, for example;
  - verifying representations and claims made by the issuer that are crucial to the performance of the offering (*e.g.*, costs projected to execute the business plan, projected timing, overall rate of return for investors);
  - identifying any red flags with the offering or the issuer, such as questionable business plans or unlikely projections or results; and
  - identifying concerns that would be deemed material to a potential investor, such as liquidity restrictions.
- *Review of Offering Terms:* Reviewing offering terms to determine if they are reasonably structured for compliance with applicable rules (*e.g.*, the escrow arrangements and termination provisions in contingency offerings) **and evaluating whether projected returns stated in offering documents are consistent with the overall financial structure and fundamentals of the offering and issuer.**
- ***Ongoing Use of Proceeds Assessment:* Maintaining a reasonable understanding of** material changes to the offering—or the issuer's business during the offering—and evaluating factors that may alter the issuer's intended use of proceeds.

### Additional Resources

- FINRA
  - Private Placements Key Topics Page
  - SEC Regulation Best Interest Key Topics Page
  - Report Center—Corporate Financing Report Cards
  - *Regulatory Notice 23-08* (FINRA Reminds Members of Their Obligations When Selling Private Placements)
- SEC
  - Regulation Best Interest, Form CRS and Related Interpretations
  - Disqualification of Felons and Other "Bad Actors" from Rule 506 Offerings and Related Disclosure Requirements (Sept. 19, 2013)

## ANNUITIES SECURITIES PRODUCTS

### Regulatory Obligations

The SEC's Reg BI[30] 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 recommendations of variable annuities and RILAs.

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 **when making a recommendation**. The standard of conduct established by Reg BI cannot be satisfied through disclosure alone.

In addition, FINRA Rule 2330 (Members' Responsibilities Regarding Deferred Variable Annuities) continues to apply to recommended purchases and exchanges of deferred variable annuities (referred to below as "variable annuities"). FINRA Rule 2330, among other things, requires member firms to establish and maintain specific written supervisory procedures reasonably designed to achieve compliance with the rule. Member 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.

### Findings

- *WSPs:* Failing to have **reasonably designed written** supervisory procedures to achieve compliance with FINRA Rule 2330 or reasonably designed written policies and procedures to **achieve compliance with** Reg BI, as applicable, with respect to:
  - recommendations of **variable** annuities **or RILAs** to help ensure that customers are not over-concentrated in variable annuities or RILAs in light of their holdings in other illiquid asset classes;

- consideration of the customer's age in assessing whether the recommendation to purchase an annuity **complies with FINRA Rule 2330 or Reg BI**;
- recommendations related to issuer buyout offers (*e.g.*, registered representatives' recommendations that investors surrender the contract pursuant to an insurance company's offer to generate an exchange or new purchase);
- registered representatives' recommendations of additional deposits into existing variable annuity contracts, including review of any applicable disclosure, new surrender periods related to this transaction and rationale for the addition;
- detecting rates of exchanges that may indicate a violation of FINRA Rule 2330 or Reg BI (*e.g.*, recommending the same replacement of a variable annuity to many customers with different investment objectives); and
- conducting training for registered representatives and supervisors regarding how to assess and compare costs and fees, surrender charges, and long-term income riders to determine whether exchanges complied with the standards of FINRA Rule 2330 and Reg BI.

- *Exchanges:* Recommending variable annuity exchanges that **did not comply with FINRA Rule 2330 or** were not in the best interest of retail customers where the exchanges were inconsistent with the customer's investment objectives and time horizon and resulted in, among other consequences:
  - increased mortality and expense, administration and rider fees to the customer;
  - the imposition of surrender fees for early liquidation of the customer's existing product**;** or
  - the loss of material benefits (*e.g.,* loss of a living benefit rider).
- *Reg BI Care Obligation Violation **in Connection with** Recommended Surrenders/Withdrawals:*
  - recommending without a reasonable basis that customers surrender existing **variable** annuities **or RILAs** and then use the proceeds to purchase RILAs;
  - **failing to consider the costs of terminating variable annuity living benefits and features, such as living benefit riders, when recommending a replacement or exchange; and**
  - **recommending partial withdrawals or full surrenders from RILAs "mid-segment" without considering interim value risk.**[31]
- *Reasonably Available Alternatives:* Pursuant to Reg BI, insufficient consideration of reasonably available alternatives to the recommended annuity purchase, surrender or exchange.
- *False or Misleading Documentation:* Submitting paperwork for recommended variable annuities **or RILA** transactions that contain misrepresentations or omissions (*e.g.*, falsely stating the transaction was not funded by another variable annuity; understating surrender charges; not indicating when customers had surrendered or exchanged a variable annuity in the past 36 months).
- *Poor and Insufficient Data Quality:* Not collecting and retaining records on annuity transactions, particularly in connection with replacement/exchange transactions; relying on processes for data collection and retention in situations where the volume of annuity transactions renders these processes ineffective; and failing to address inconsistencies in available transaction data for **variable** annuities **or RILAs** (*e.g.*, with respect to identifying and labeling replacements/exchanges), as well as data formats and reporting processes.

## Effective Practices

- *Applying **FINRA Rule 2330's** Heightened Policies and Procedures to RILA Recommendations:* **As an effective practice**, incorporating into a firm's WSPs and written policies and procedures heightened policies and procedures for recommendations of RILAs, such as the explicit requirements that apply to **recommendations of deferred** variable annuities under FINRA Rule 2330, including, but not limited to requiring:
  - a registered representative to document and sign his or her rationale for a recommendation of a RILA based on the client's specific needs and investor profile;
  - a registered principal to review and determine whether he or she approves of a recommended purchase or exchange of a RILA;
  - a **registered** principal **(who reviews the transaction)** to document and sign the basis for his or her approval (or rejection) of the recommendation;
  - the gathering of information regarding whether customers have had RILA exchanges (or replacements of VAs with RILAs and vice versa) within the preceding 36 months; and
  - implementation of surveillance procedures to determine if any of the firm's associated persons have rates of effecting RILA exchanges (or replacements of VAs with RILAs and vice versa) that raise for review whether such exchanges evidence conduct inconsistent with Reg BI.
- *Addressing RILA Features:* Providing guidance to associated persons on how to consider whether RILAs (including investment options) and particular features of a RILA are in a retail customer's best interest, including:
  - the manner in which interest is calculated and credited;
  - the bounded return structure;
  - automatic renewals that occur at the end of a crediting period; and
  - applicable contract adjustments, including interim value adjustments (IVAs), market value adjustments (MVAs) or limits on the RILA's performance.
- *Exchange Disclosures:* Using exchange disclosure forms to provide the customer with meaningful information about the advantages and disadvantages of the recommended exchange, including:
  - a comparison of the fees (and in the case of RILAs, the economic costs of their bounded return structure as well as IVAs and MVAs) and surrender periods of the existing and new products;
  - disclosure of the loss of any benefits with the existing product (including a benefit base that exceeds the contract value); and
  - the representative's rationale for the exchange.
- *Account Recommendations:* Providing guidance on how to consider account types and costs when potentially recommending broker-dealer versus advisory annuity contract classes.
- *Automated Surveillance:* Using automated tools, exception reports, and surveillance to review exchanges **of variable annuities or RILAs (including, in some cases, those that take into consideration the "cumulative surrender charges" incurred by customers of a particular**

**associated person over a given period and excessive rates of exchanges within the last one to two years of the surrender schedule);** and implementing second-level supervision of supervisory reviews of exchange-related exception reports and account applications.

- *Detailed Rationales for Exchanges:* Confirming that registered representatives'—and, where applicable, **registered** principals'—written rationales for exchanges for each customer address the specific circumstances for each customer and **are not generic or insufficient**; and requiring **registered** principals to verify the information in these rationales that registered representatives provide, including product fees, costs, rider benefits and existing product values.
- *Review Thresholds:* Standardizing review thresholds for rates of exchanges; and monitoring for emerging trends across registered representatives, customers, products and branches.
- *Data Integrity:* Engaging with insurance carriers (affiliated and non-affiliated) and third-party data providers (*e.g.*, Depository Trust and Clearing Corporation (DTCC), consolidated account report providers) to confirm their data integrity (including general product information, contract class, riders and exchange-based activity).
- *Data Acquisition:* Establishing a supervisory system that collects and uses key transaction data **to supervise transactions and identify patterns.**
- *Data Analysis:* Considering the following data points when conducting a review of a recommended 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
  - whether the customer has had another exchange within the preceding 36 months
  - living benefit value, death benefit value or both, that was forfeited
  - surrender charges incurred
  - any additional benefits surrendered with forfeiture

## Additional Resources

- FINRA
  - Variable Annuities Key Topics Page
  - SEC Regulation Best Interest Key Topics Page
  - The Reg BI and Form CRS topic
  - *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)

- SEC
  - Registration for Index-Linked Annuities and Registered Market Value Adjustment Annuities, Final Rule, Securities Act Release No. 33-11294 (July 1, 2024), 89 FR 59978 (July 24, 2024)
  - Registration for Index-Linked Annuities; Amendments to Form N-4 for Index-Linked and Variable Annuities, Proposed Rule, Securities Act Release No. 11250 (Sept. 29, 2023), 88 FR 71088 (Oct. 13, 2023).
  - Investor Testing Report on Registered Index-Linked Annuities (September 2023)
  - Regulation Best Interest, Form CRS and Related Interpretations

# Market Integrity

## CONSOLIDATED AUDIT TRAIL

### Regulatory Obligations

Rule 613 under Regulation NMS required FINRA and the national securities exchanges to jointly submit a National Market System (NMS) plan detailing how they would develop, implement and maintain a consolidated audit trail that collects and accurately identifies every order, cancellation, modification and trade execution for all equities and exchange-listed options across all U.S. markets. FINRA and the national securities exchanges filed the NMS plan and the plan was approved and is now effective.

FINRA and the national securities exchanges have adopted rules requiring their members to comply with SEA Rule 613 and the CAT NMS Plan, 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) notes that firms' WSPs also must be reasonably designed to ensure that the data reported by them or on their behalf is transmitted in a timely fashion and that it is complete and accurate.

#### Customer and Account Information System (CAIS) Reporting Obligations (Updated for 2026)

- On Feb. 10, 2025, the SEC issued an order providing exemptive relief related to the reporting of certain customer information to CAIS for Designated Natural Persons. CAT Alert 2025-02 provides guidance on the application of the SEC's CAIS Exemption Order and reporting alternatives of Industry Members who choose to continue reporting names, addresses and years of birth for Designated Natural Persons.
- On March 13, 2025, CAT LLC filed with the SEC a proposed amendment to the CAT NMS Plan related to further changes to CAIS ("CAIS Amendment").[32] If approved, the CAIS Amendment would eliminate requirements that Industry Members report customer names, customer addresses, and years of birth for natural persons with transformed SSNs or ITINs; natural persons without transformed SSNs or ITINs; and legal entities.
- There may be additional changes proposed to CAT, which could further impact member firms' reporting requirements. Firms can find the latest updates and additional information related to CAIS reporting and the CAIS Amendment on the CAT NMS Plan website.

## Findings

- *Incomplete Submission of Reportable Events:* Failing to report certain Reportable Events, as defined by CAT, in a timely manner to the Central Repository (*e.g.*, new order events, route events, execution events).
- *Failure to Repair Errors Timely:* Not repairing errors by the T+3 correction deadline.
- *Failure to Submit Corrections:* Not submitting corrections for previously inaccurately reported data, including data that did not generate error feedback from CAT.
- *Inaccurate or Incomplete Reporting of CAT Orders:* Submitting information that was inaccurate, incomplete or both to the Central Repository.
- *Unreasonable Supervision:*
  - Not establishing and maintaining reasonable WSPs or supervisory controls regarding CAT reporting and clock synchronization performed by the firm, third-party vendors, or both.
  - Not implementing an accuracy review as described in the **"Specific Consideration for CAT Supervisory Systems and Procedures"** in *Regulatory Notice* 20-31 (FINRA Reminds Firms of Their Supervisory Responsibilities Relating to CAT).
  - Not using a reasonable sample size when selecting firm CAT reports for review.
  - **Not using a sample with a variety of order and event types when selecting firm CAT reports for review.**
  - **Not using a proportionate sample of all desks, aggregation units, business lines and types of order flow from across the firm when reviewing for reporting accuracy.**
  - Not **reasonably** supervising Reporting Agents that report to CAT on the firm's behalf.
  - Not promptly remediating CAT reporting issues when brought to the firm's attention either through its own reviews or regulatory inquiries from FINRA.
- *Recordkeeping:* Not maintaining underlying books and records to support transactional data reported to CAT.

## Effective Practices

- *Mapping Internal Records to CAT-Reported Data:* Maintaining a "map" that shows how the firm's internal records and blotters correspond to various fields reported to CAT.
- *Archiving CAT Feedback:* Archiving CAT feedback within a 90-day window so that firms can submit corrections, if necessary.
- *CAT Supervision:* Implementing WSPs requiring a comparative review of CAT submissions versus firm order and trade records (including for firms that rely on third-party submitters); conducting a daily review of the CAT Reporter Portal, regardless of the error rate percentage; utilizing CAT Report Cards and CAT FAQs to design an effective and reasonable supervision process; and, when relying on a CAT reporting agent, maintaining a written agreement that specifies the respective functions and responsibilities for exception management and error correction.

- *CAT Clock Synchronization:* When relying on third-party, non-broker-dealer vendors for synchronization of business clocks, obtaining synchronization logs daily from such parties and reviewing them to ensure that the clock drifts are within acceptable thresholds (*i.e.*, 50 milliseconds).[33]
- *Supervision of Transformed Identifier and FDID Reporting:* Establishing reasonable supervisory processes and procedures that address monitoring that customer and account information is reported in an appropriately secure manner pursuant to CAT reporting requirements (*e.g.*, customer identifiers are not submitted to CAT or CAIS unless they have been properly transformed into a "hashed" Transformed Input ID (TID) prior to submission; customer account identifiers (FDIDs) do not reflect actual account numbers).
- *Self-Reporting:* Self-reporting CAT or CAIS reporting issues via the appropriate form (available in the Forms section of the CAT NMS Plan website) or through the FINRA CAT Help Desk.

### Additional Resources

- FINRA
  - Consolidated Audit Trail (CAT) Key Topics Page
  - *Regulatory Notices*
    - *Regulatory Notice 20-41* (FINRA Amends Its Equity Trade Reporting Rules Relating to Timestamp Granularity)
    - *Regulatory Notice 20-31* (FINRA Reminds Firms of Their Supervisory Responsibilities Relating to CAT)
    - *Regulatory Notice 17-09* (The National Securities Exchanges and FINRA Issue Joint Guidance on Clock Synchronization and Certification Requirements Under the CAT NMS Plan)
  - **CAT Alert 2025-02: Update Regarding SEC's CAIS Exemption Order**
  - CAT NMS Plan Website
  - CAT NMS Clock Synchronization

## CUSTOMER ORDER HANDLING: BEST EXECUTION AND ORDER ROUTING DISCLOSURES

### 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 firm and persons associated with a 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. A firm must have procedures in place to ensure it conducts "regular and rigorous" reviews of the execution quality of its customers' orders if it does not conduct an order-by-order review. MSRB Rule G-18 (Best Execution) sets forth similar obligations with respect to transactions in municipal securities. In addition, the SEC has interpreted the antifraud provisions to require broker-dealers to provide best execution, and the SEC has interpreted that obligation in particular circumstances.

Best execution obligations apply to any firm that receives customer orders for purposes of handling and execution, including firms that receive customer orders from other firms for handling and execution.[34] These obligations apply whether a firm acts in a principal or in an agency capacity. A firm cannot transfer its duty of best execution to another person. Additionally, a firm that routes **its order flow** to another firm **that has agreed to handle that order flow as agent for the customer** must either conduct its own regular and rigorous review of the execution quality received, or periodically review the statistical results and rationale of the other firm's regular and rigorous review of execution quality.

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. **FINRA Rule 6151 requires members to submit their Rule 606 order routing reports to FINRA for centralized publication on the FINRA website.**

## Findings

*Best Execution*

- *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, including ATSs and additional sources of liquidity; failing to modify routing arrangements or justify why routing arrangements are not being modified; and using routing logic that is not based on execution quality.
- *Unreasonable "Regular and Rigorous Reviews":* Not conducting periodic "regular and rigorous reviews" or, when conducting such reviews, not considering certain execution quality factors set forth in FINRA Rule 5310, Supplementary Material .09.
- *No Review of Certain Order Types:* Not conducting adequate reviews on a type-of-order basis, including, for example, for market, marketable limit, or non-marketable limit orders.
- *Securities with Limited Quotations or Pricing Information:* Failing to establish **written policies and** procedures with respect to trading in securities with limited quotations or pricing information as set forth in FINRA Rule 5310, Supplementary Material .06, including documenting compliance with those policies and procedures.

*Order Routing Disclosures*

- *Inaccurate Quarterly Reports:* Publishing incomplete or otherwise inaccurate information in the quarterly report on order routing, such as:
  - inaccurately classifying orders (*e.g.*, classifying orders as "other orders" without considering whether such orders involve a customer request for special handling);[35]
  - incorrectly stating that the firm does not receive payment for order flow (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);
- reporting only held orders in listed options, instead of both held and not held orders; and
- inaccurately identifying reported execution venues as "Unknown."

- *Incomplete Disclosures:* Not adequately describing material aspects of the firm's 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);
  - incomplete descriptions of exchange credits or rebates; and
  - incomplete descriptions of tiered pricing arrangements, including the specific pricing received by the firm.
- *Insufficient WSPs:* Either not establishing or not maintaining WSPs reasonably designed to achieve compliance with the requirements of Rule 606, including:
  - not describing the steps taken to review whether the firm has verified the integrity of information sent to, or received from, their third-party vendor—or not stating how the review would be evidenced;
  - not articulating a supervisory method of review to verify the accuracy, format, completeness, timely processing, and details of the Rule 606(b)(1) and (b)(3) reports, if requested, as well as documenting the performance of that review; and
  - when incorporating by reference another firm's Rule 606(a)(1) quarterly report, not examining the report and having a reasonable basis to believe that the report does not materially misrepresent the order routing practices.

## Effective Practices

*Best Execution*

- *Supervision of Order Flow:* Ensuring supervisory procedures, systems and controls address the execution of the entirety of the firm's marketable order flow, including order types such as activated stop orders, all or none orders, and odd lot orders.

- *Monitoring Orders:*
  - Monitoring the handling of marketable orders of all types fully and promptly, including market orders, marketable limit orders, activated stop orders, all or none orders, odd lot orders, marketable orders in illiquid securities and marketable orders in preferred securities.
  - **For firms relying** on the regular and rigorous review of execution quality conducted by an executing firm, consolidator or other **member that has agreed to handle the firm's order flow as agent for the** customer:
    - ensuring that the statistical results and rationale of the executing firm's, consolidator's or other **member firm's** review are fully disclosed to **the firm**; and
    - periodically reviewing both the methodology and the results of the review.
- *Exception Reports:* Using exception reports and surveillance reports to support the firm's efforts to meet their best execution obligations.
- *Full and Prompt Execution of Marketable Customer Orders:* Regularly evaluating the firm's thresholds used to generate exceptions as part of the firm's supervisory systems designed to achieve compliance with the firm's "full and prompt" obligations; and modifying such thresholds to reflect current promptness standards for marketable order execution, including statistics available from FINRA, other relevant indicators of industry standards, and the firm's internal data.
- *PFOF Order Handling Impact Review:* Reviewing how PFOF affects the firm's order-handling process, including:
  - any explicit or implicit contractual arrangement to send order flow to a third-party broker-dealer;
  - the 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 on a quarterly or more frequent basis (such as monthly), depending on the firm's business model, that consider the potential execution quality available at various **market** centers**, including competing markets** to which a firm does not send order flow.
- *Support of Analysis:* Being prepared to explain and evidence the firm's best execution analysis, including internalized orders, on a "regular and rigorous" or order-by-order basis, as applicable.
- *Continuous Updates:*
  - Updating WSPs and best execution analysis to address market and technology changes.
  - Maintaining and regularly reviewing firm policies and procedures to comply with FINRA Rule 5310 and updating or revising such policies and procedures, as necessary.
- *Best Execution Committees:* Establishing committees that meet quarterly or more frequently to conduct "regular and rigorous" reviews and determine, if necessary, to modify the firm's order routing and execution arrangements.

*Order Routing Disclosures*

- *Supervision:* Conducting regular, periodic supervisory reviews to ensure that:
  - public quarterly reports and customer-specific order disclosure reports are:
    - accurate (*e.g.*, assuring that per-venue disclosures of net aggregate PFOF and other payments are accurately calculated); and
    - complete (*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); and
  - SEC Rule 606(a) Reports are provided to FINRA, in the manner prescribed by FINRA, within the same time and in the same formats that such report is required to be made publicly available pursuant to Rule 606(a), and that:
    - erroneous or rejected submissions to FINRA are corrected and resubmitted;
    - hyperlinks in reports submitted to FINRA are operational;
    - reports made publicly available by firms are consistent with the reports submitted to FINRA; and
    - complete and current clearing firm information is submitted to FINRA (for introducing firms that incorporate by reference their clearing firm(s)' Rule 606(a) Reports).
- *Due Diligence:*
  - *Identifying Execution Venues:* Routing-only firm (*i.e.*, a broker-dealer that re-routes but does not execute orders) confirming it is not inaccurately reported as an execution venue.
  - *Third-Party Vendors:* Assess the accuracy of public quarterly reports and customer-specific order disclosure reports provided by third-party vendors by, for example:
    - reviewing the content of reports; and
    - comparing order samples against third-party vendor-provided information, and confirming with the third-party vendor that all appropriate order information is being received (particularly when the firm has complex routing arrangements with execution venues).

## Additional Resources

- FINRA
  - Report Center
    - Best Execution Outside-of-the-Inside Report Card
    - Equity Report Cards
    - Market Order Timeliness Statistical Report
  - FINRA Rule 6151 (Centralization of SEC Rule 606(a) Reports)
  - *Regulatory Notices*
    - *Regulatory Notice 24-05* (FINRA Adopts Amendments to Improve the Accessibility of Order Routing Disclosures for NMS Securities)
    - *Regulatory Notice 22-04* (FINRA Reminds Member Firms of Obligation to Execute Marketable Customer Orders Fully and Promptly)

- *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 Firm Best Execution Obligations And Provides Guidance to Members Concerning Compliance)

- SEC
  - Responses to Frequently Asked Questions Concerning Rule 606 of Regulation NMS (updated June 26, 2024)
  - Division of Examinations Risk Alert: Observations Related to Regulation NMS Rule 606 Disclosures (Nov. 10, 2022)
  - SEC Adopts Rules That Increase Information Brokers Must Provide to Investors on Order Handling (Nov. 2, 2018)

## FIXED INCOME—FAIR PRICING

### Regulatory Obligations

The fair pricing obligations under FINRA Rule 2121 (Fair Prices and Commissions) apply to transactions in all securities—including fixed income securities—and MSRB Rule G-30 (Prices and Commissions) imposes similar obligations for transactions in municipal securities.

These rules generally require a dealer that is acting in a principal capacity in a debt security transaction with a customer, and charging a mark-up or mark-down, to mark up or mark down the transaction from the prevailing market price (PMP). The PMP is presumptively established by referring to the dealer's contemporaneous cost as incurred or proceeds as obtained. Where the dealer's cost is no longer contemporaneous, or the dealer has overcome the contemporaneous cost presumption, firms are required to continue down the "waterfall" within FINRA Rule 2121 or MSRB Rule G-30, as applicable, to determine the PMP.

### Findings

- *Incorrect Determination of PMP:* Not following the contemporaneous cost presumption or the waterfall required by FINRA Rule 2121 and MSRB Rule G-30, but rather:
  - using other methods, such as obtaining quotations from a limited number of market participants without considering contemporaneous inter-dealer or institutional transaction prices;

- referring to acquisition costs that are no longer contemporaneous;
- relying on third-party software to determine the PMP, while:
  - not understanding how the software determines the PMP, notwithstanding the firm's ultimate responsibility for ensuring the PMP is determined in accordance with FINRA Rule 2121 and MSRB Rule G-30;
  - not ensuring that the software could access all information necessary to properly determine the PMP (*e.g.*, the feed of the firm's own trading was incomplete); or
  - **not subsequently considering trades flagged by the software for compliance or supervisory review based on the amount of mark-up or mark-down from the determined PMP;**
- permitting registered representatives to determine the PMP through a manual override of the third-party software, while:
  - not appropriately supervising how the PMP was determined in manual overrides;
  - not maintaining documentation regarding why manual override was necessary or how the PMP was determined in manual overrides; or
- determining the PMP based on the firm's quotation prices, rather than determining the PMP in accordance with the waterfall **(*e.g.*, incorrectly categorizing the firm's quotation price as the contemporaneous cost/proceeds level of the waterfall when determining the PMP).**

- *Outdated Mark-Up/Mark-Down Grids:* Employing mark-up/mark-down grids without periodically reviewing and updating them as needed.
- *Failure to Consider Impact of Mark-Up on Yield to Maturity:* Charging substantial mark-ups on short-term, fixed-income securities that may significantly reduce the yield received by the investor.
- *Unreasonable Supervision:* Solely relying on grids or on fixed mark-up/mark-down thresholds in assessing fair pricing in fixed income securities without performing a facts-and-circumstances analysis as required by FINRA Rule 2121 or MSRB Rule G-30.

## Effective Practices

- *PMP Documentation:* Documenting the PMP for each transaction, even if it does not require a mark-up/mark-down disclosure pursuant to FINRA Rule 2232 (Customer Confirmations) or MSRB Rule G-15 (Confirmation, Clearance, Settlement and Other Uniform Practice Requirements with Respect to Transactions with Customers).
- *Mark-Up/Mark-Down Reviews:* Conducting periodic reviews of the firm's mark-ups/mark-downs and comparing them with industry data provided in the TRACE and MSRB Mark-Up/Mark-Down Analysis Reports.
- *Exception Reports:* Using exception reports or outside third-party vendor software, and periodically reviewing and updating the reports' parameters so they perform as intended, even as market conditions change.

- *Considering the Cumulative Customer Impact of Proceeds Transactions:* When using the proceeds from a customer sale of bonds to purchase new bonds for the customer at or **near** the same time, **taking into account** both the mark-down on the sale and the mark-up on the purchase **in considering the total charges borne by the customer.**

### Additional Resources

- FINRA
  - FINRA Data
    - Fixed Income Data
  - Fixed Income Confirmation Disclosure: Frequently Asked Questions (FAQ) Key Topics Page
  - MSRB Markup/Markdown Analysis Report
  - TRACE Markup/Markdown Analysis Report
  - *Regulatory Notices*
    - *Regulatory Notice 21-29* (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors)
    - *Regulatory Notice 17-08* (SEC Approves Amendments to Require Mark-Up/Mark-Down Disclosure on Confirmations for Trades With Retail Investors in Corporate and Agency Bonds)
- MSRB
  - Resource on Disclosing Mark-ups and Determining Prevailing Market Price (July 2018)
  - Confirmation Disclosure and Prevailing Market Price Guidance: Frequently Asked Questions (March 19, 2018)

## MARKET ACCESS RULE

### Regulatory Obligations

SEA Rule 15c3-5 (Market Access Rule) requires firms with market access or that provide market access to their customers or any other person 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, ETFs, debt securities, security-based swaps and security futures products.

### Findings

- *Insufficient Controls:*
  - Not establishing **reasonable** pre-trade order limits, preset capital **and credit** thresholds, and duplicative and erroneous **pre-trade** order control **thresholds** for accessing **exchanges and** ATSs, including those that **trade** fixed income **securities**.
  - Setting pre-trade financial capital and credit and duplicative and erroneous limits at unreasonable thresholds based on a firm's business model.

- Not demonstrating and failing to maintain documentation demonstrating the reasonability of assigned capital, credit and erroneous order pre-trade financial controls.
- Not establishing adequate 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, or documenting justifications for any adjustments and ensuring thresholds for temporary adjustments to revert to their pre-adjusted values.
- Overly relying on multiple, stand-alone risk management control systems, and failing to consider market access controls in the aggregate (*e.g.,* failing to assess excessive messaging across different ports and venues for a given customer).

- *Failure to Consider Additional Data:* Failing to consider a firm's business model when setting pre-trade order limits or other regulatory requirements (*e.g.*, Limit Up-Limit Down (LULD) thresholds, exchanges' Limit Order Price Protection thresholds), as well as historical and available liquidity and the time required for liquidity replenishment when determining erroneous price and size control thresholds.
- *Impermissible Exclusions:* Excluding certain orders from a firm's pre-trade erroneous controls based on order types (*e.g.*, excluding limit on close**, market maker peg orders or other aggressively priced order types from a firm's price controls).**
- *Inadequate Financial Risk Management Controls:* For firms with market access, or those that provide it, having unreasonable capital thresholds for trading desks and unreasonable aggregate daily limits or credit limits for institutional customers and counterparties.
- *Reliance on Third-Party 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 third-party vendors' controls operate, or both; and not maintaining direct and exclusive control over controls by allowing the ATS **or exchange** to unilaterally set financial thresholds for firms' orders without the involvement of the firm, instead of establishing their own thresholds.
- *Inadequate Post Trade Surveillance:* Failure to conduct post trade reviews for potential manipulation.
- *Failure to Document Annual Review of Effectiveness:* Failure to document the firm's review, conducted at least annually, of the effectiveness of its risk management controls and supervisory procedures (*e.g.*, no inventory of the specific systems, controls, thresholds or functionality that were reviewed), including the reasonableness of the firm's market access controls applicable to each business/product line in which the firm provides market access.

## 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.

- *Soft Blocks:*
  - Implementing detailed and reasonable WSPs that list the steps that firm personnel should take when determining how to handle orders that trigger soft controls; and requiring staff to document their findings and rationale for releasing an order following a review.
  - Conducting a separate supervisory review to ensure that release rationales are appropriate; and requiring the incorporation of review results when assessing the effectiveness of the firm's controls.
- *Tailored Controls to Prevent Erroneous or Duplicative Orders:*
  - Tailoring controls to prevent erroneous or duplicative orders to particular products, situations (*e.g.,* corporate actions), or order types; and preventing the routing of market orders based on impact (*e.g.,* 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.
  - Ensuring that controls apply to all order flow and all trading sessions.
- *Market Impact:* Developing reasonable complementary controls (*e.g.*, a market impact check, a liquidity check, an average daily volume control) based upon the firm's business model and historical order flow; and using a benchmark when pricing child orders for a larger parent market order (*e.g.*, the National Best Bid and Offer (NBBO) or last sale at the time of the initial child order route) to monitor the cumulative market impact of subsequent child orders over a short period of time.
- *Reference Data:* Using a reasonable process for choosing reference data in developing various controls, so if one piece of data is not obtained another could be substituted (*e.g.*, the NBBO versus the last sale or the previous day's closing price).
- *Post-Trade Controls and Surveillance:* When providing direct market access via multiple systems, including sponsored access arrangements, employing reasonable controls to confirm that the 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 **and, if applicable, compliance with Regulation NMS.**
- *Testing of Risk Management Controls:* Regularly testing market access controls, such as:
  - performing a review, at least annually, of the business activity of the firm in connection with market access;
  - maintaining data and documents that evidence the rationale for continued use of implemented controls and parameters;
  - focusing on the parameters for controls and analyzing whether they are reasonable and would prevent the entry of erroneous orders under different scenarios (*e.g.*, the entry of a large order in a thinly traded or high-priced security) and product types;
  - determining whether hard blocks are working (*e.g.*, triggered when a parameter is triggered);

- documenting reviews and retaining information used in decisions to adjust, maintain or create new controls (*e.g.*, change in business lines may result in short period-of-time controls in addition to order-by-order controls);
- reviewing any automated controls to timely revert *ad hoc* credit limit adjustments; and
- for firms that provide clients sponsored access, verifying ability to retain direct and exclusive control over the pre-trade financial and regulatory requirements.

- *Training:* Conducting training for individual traders regarding the steps and requirements for requesting *ad hoc* credit limit adjustments, **or when to release an order triggered by a soft block.**

### Additional Resources

- FINRA
  - Algorithmic Trading Key Topics Page
  - Market Access Key Topics Page
  - *Regulatory Notices*
    - *Regulatory Notice 16-21* (Qualification and Registration of Associated Persons Relating to Algorithmic Trading)
    - *Regulatory Notice 15-09* (Guidance on Effective Supervision and Control Practices for Firms Engaging in Algorithmic Trading Strategies)
    - *Notice to Members 04-66* (NASD Reminds Member Firms of Their Obligations to Ensure the Accuracy and Integrity of Information Entered into Order-Routing and Execution Systems)
- SEC
  - Responses to Frequently Asked Questions Concerning Risk Management Controls for Brokers or Dealers with Market Access (April 15, 2014)

## EXTENDED HOURS TRADING

### Regulatory Obligations

Firms that participate in extended hours trading must comply with FINRA Rule 2265 (Extended Hours Trading Risk Disclosure), as well as with other FINRA and SEC rules applicable to such trading, including without limitation FINRA Rule 5310 (Best Execution and Interpositioning), and must ensure they meet their supervisory obligations for extended hours activity under FINRA Rule 3110 (Supervision).

FINRA Rule 2265 requires that firms that permit customers to engage in extended hours trading provide customers with a risk disclosure statement. In addition, if the firm permits customers to engage in extended hours trading online, or open accounts online in which the customer may engage in extended hours trading, the firm must post a risk disclosure statement on the firm's website in a clear and conspicuous manner. The risk disclosure must address, at a minimum, the six specific risks identified in FINRA Rule 2265, and firms must also consider whether to develop and include additional disclosures as necessary to address product-specific or other specific needs.

## Findings

- *Inadequate Supervision:* Failing to maintain reasonably designed supervisory systems and controls, including with respect to the identification and reporting of potentially manipulative activity conducted in after-hours trading.[36]
- *Reporting Failures:* Failing to report to FINRA's Trade Reporting Facilities (TRF) or CAT required information arising from activity conducted during extended hours trading.

## Effective Practices

- *Best Execution Reviews:* Evaluating how extended hours orders are handled, routed and executed in regular and rigorous best execution reviews to confirm that the firm's practices are reasonably designed to achieve best execution.
- *Customer Disclosures:* Reviewing customer disclosures about the risks of extended hours trading to ensure that such disclosures address, at a minimum, the risks enumerated in FINRA Rule 2265; evaluating whether any additional product-specific or other disclosures may be necessary to address other risks related to extended hours trading; and reviewing any customer disclosures about the firm's customer order handling procedures.
- *Supervisory Processes:*
  - Establishing and maintaining reasonably designed supervisory processes that address any unique characteristics or risks of extended hours trading, such as customer order handling and volatile or illiquid market conditions.
  - **Establishing reasonably designed supervisory processes that account for the mechanics and unique characteristics of overnight trading—such as venue-specific overnight price bands—and that contemplate supervisory reviews for scenarios that appear to reflect trades outside the bands, or trades that appear designed to set the bands in a potentially manipulative manner.**
- *Operational Readiness, Customer Support and Business Continuity Planning:* Evaluating unique operational readiness and customer support needs during overnight hours, as well as the availability of backup trading arrangements during trading sessions that are offered to customers and considering appropriate communications with customers about potential service interruptions.

## Additional Resources

- FINRA
  - Investor Insights—Extended-Hours Trading: Know the Risks (July 31, 2024)
  - *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)

# Financial Management

## NET CAPITAL

### Regulatory Obligations

SEA Rule 15c3-1 (Net Capital Rule) requires that firms must at all times 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. SEA Rule 17a-11 requires firms to notify FINRA and the SEC when their net capital falls below the required minimum amount.

To assist firms in complying with SEA Rule 15c3-1, FINRA has published ***Regulatory Notice 25-12*** **(FINRA Announces Update of the Interpretations of Financial and Operational Rules)**, *Regulatory Notice 23-21* (FINRA Reminds Member Firms of Net Capital, Recordkeeping and Financial Reporting Requirements in Connection with Revenue Recognition Practices) and *Notice to Members 03-63* (SEC Issues Guidance on the Recording of Expenses and Liabilities by Broker/Dealers). *Regulatory Notice 23-21* advises firms to ensure that they can demonstrate their proper application of the Financial Accounting Standards Board's (FASB) Topic 606 (Revenue from Contracts with Customers), which serves as a foundation for compliance with the Net Capital Rule, SEA Rule 17a-3 and SEA Rule 17a-5.

If firms have an affiliate or parent paying any of their expenses, FINRA *Notice to Members 03-63* provides guidance for establishing an expense-sharing agreement.

#### SEC Division of Trading and Markets Publishes FAQ Related to Crypto Assets

- The SEC's Division of Trading and Markets published FAQs relating to crypto asset activities and distributed ledger technology and withdrew the 2019 Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities.
- The FAQs address several financial responsibility rules. In relation to addressing whether a broker-dealer is prohibited by custody and capital requirements from facilitating in-kind creations and redemptions in connection with a spot crypto exchange-traded product (ETP), an FAQ states that the SEC staff will not object if a broker-dealer treats a proprietary position in bitcoin or ether as being readily marketable for purposes of determining whether the 20 percent haircut applicable to commodities under Appendix B of Rule 15c3-1 applies.

## Findings

- *Improper Recording and Accrual of Revenues and Expenses:*
  - Not recording transactions in a timely manner, or maintaining financial records on an accrual basis resulting in the firm's noncompliance with SEA Rule 17a-3.
  - **Not keeping accurate books and records (*e.g.,* FOCUS filings, general ledgers) and not correctly classifying or accruing expenses and related liabilities, thereby leading to inaccurate net capital computations.**
- *Inadequate Processes or Supervision Concerning Net Capital Deductions:* Not maintaining a process or WSPs to accurately compute capital charges of nonmarketable securities (*e.g.*, failing to compute marketplace blockage properly); and for certain firms, applying **the lower haircuts only afforded to securities with a** "minimal amount of credit risk" despite not having an adequate process to assess the creditworthiness of the security.
- *Inadequate Supervision of Net Capital Compliance:* Not having a reasonable process to determine when the firm has a net capital deficiency **and should take appropriate regulatory action such as file timely notification of** its net capital deficiencies and begin the process of suspending business operations.
- *Late or Inadequate Filings:* Failing to timely file required notices of net capital deficiencies with FINRA and the SEC.
- *Inadequate Processes or Supervision Concerning Capital Charges for Underwriting Commitments:* Not maintaining an adequate process to assess moment-to-moment net capital and open contractual commitments (OCC) capital charges on underwriting commitments; not establishing and maintaining WSPs for calculating and applying OCC charges; not maintaining an accurate record or log of underwritings in which the firm is involved; not understanding the firm's role in the underwriting (*i.e.*, best efforts or firm commitment); **and not properly documenting that the commitment has been fully sold before discontinuing the OCC charges.**
- *Insufficient Capital for Underwriting Participation:* Acting in the capacity as the lead underwriter without maintaining sufficient minimum net capital to participate in such underwriting capacity and cover the required OCC charges.
- *Inaccurate OCC Charges:* Failing to accurately capture OCC charges on firm commitment offerings (*e.g.*, only capturing charges for the day of the pricing date or the settlement date, not capturing charges on unsold portion of underwriting from pricing date through settlement date, applying an incorrect haircut percentage **as the open contractual commitment deduction).**

## Effective Practices

- *Net Capital Assessment:* Performing an ongoing assessment of the net capital treatment of assets to confirm that they were correctly classified **as allowable** for net capital purposes.
- ***Revenue Recognition Documentation:* Documenting and consistently applying clear policies and analyses that demonstrate how the firm's revenue recognition practices comply with ASC 606 requirements.**

- *New or Complex Transaction Considerations:* **Including input from the firm's regulatory reporting staff and FINOPs (including outsourced FINOPs) as a firm looks to enter into a new or complex transaction that may lead to significant downstream impacts to the firm's Net Capital.**
- ***Moment-to-Moment and Net Capital Compliance for Underwriting Commitments:***
  - *Establishing control processes and maintaining current WSPs for:*
    - ensuring the firm's role **in a particular underwriting** is clear within the agreement (*i.e.*, best efforts or firm commitment offering);
    - establishing a process to track open contractual commitments in which the firm is currently involved;
    - calculating and applying OCC charges, as well as focusing on the product and proper haircut percentage and undue concentration charges; **and**
    - **maintaining appropriate records to evidence the firm's open contractual commitment has been extinguished and that the firm no longer is required to take an OCC charge.**

## Annual Financial Reporting Reminders and Updates for Member Firms

**SEA Rule 17a-5(d) Annual Reports:**

- Oath or affirmations must be administered by authorized persons per SEA Rule 17a-5(e)(2)(ii).
- Compliance reports (SEA Rule 17a-5(d)(3)) or exemption reports (SEA Rule 17a-5(d)(4)) must be executed by the person making the oath or affirmation.
- FASB Update 2023-07 (November 2023): All broker-dealers filing reports with SEC are "public business entities" and must apply segment disclosure guidance. Compliance date: Fiscal years that began after Dec. 31, 2023.
- Annual reports must include all required U.S. GAAP footnote disclosures (*e.g.*, ASC 606 revenue recognition, going concern, loss contingency).
- SEA Rule 17a-5(f)(3) applies when engaging or changing independent public accountants.

**Resources:**

- SEA Rule 17a-5(d) Annual reports
- Accounting Standards Update 2023-07 (Segment Reporting – ASC 280 – Improvements to Reportable Segment Disclosures)
- SEC Division of Trading and Markets Staff Guidance: Frequently Asked Questions Concerning the July 30, 2013, Amendments to the Broker-Dealer Financial Reporting Rule
- SEC Division of Trading and Markets Staff Guidance: Frequently Asked Questions Concerning the Amendments to Certain Broker-Dealer Financial Responsibility Rules

*Continued on next page*

*Continued from previous page*

- Frequently Asked Questions About Exemption Reporting Under SEA Rule 15c3-3(k) for Purposes of FOCUS Reporting and Updating of Membership Agreements

**Electronic Submission of Materials Under the SEA:**

SEC Adopts Rule Amendments for the Electronic Submission of Annual Reports and Amendments Regarding FOCUS Reports

- Annual Reports under SEA Rules 17a-5(d) must be submitted to SEC via EDGAR in PDF format for reports due on or after June 30, 2025. (Note: there are no changes to the FINRA Annual Audit Report submission process.)
- Part III of Form X-17A-5 (Annual Reports Oath or Affirmation) no longer requires notarization.
- Signatories may use manual or electronic signatures. *See* SEA Rule 17a-5(p) for electronic signature requirements.

**XBRL Implementation Timeline:**

- Firms with ≥$250,000 minimum fixed dollar net capital requirement (as of Dec. 31, 2025): XBRL format required for reports due on or after June 30, 2027
- Firms with <$250,000 minimum fixed dollar net capital requirement (as of Dec. 31, 2025): XBRL format required for reports due on or after June 30, 2029

**FOCUS Report:**

- FOCUS Part II and IIA require signature from only one principal executive officer or principal financial officer. FINOPs need not be officers to perform their role, but only officers may sign the cover page of the FOCUS report (FINOPs who are also officers may sign in their officer capacity).
- Effective March 1, 2026, the customer and proprietary accounts of broker-dealers (PAB) reserve requirement calculations will reflect SEC amendments to require daily reserve computations and Central Clearing of U.S. Treasury Securities.
- Effective March 1, 2027, the FOCUS Part II and IIA will reflect SEC amendments as adopted in the Electronic Submission of Certain Materials Under the Securities Exchange Act of 1934; Amendments Regarding the FOCUS Report.

FINRA issued *Information Notice 11/14/25* to highlight key changes and compliance dates that affect member firms.

### Additional Resources

- FINRA
  - Interpretations to the SEC's Financial and Operational Rules
  - *Regulatory Notices*
    - ***Regulatory Notice* 25-12 (FINRA Announces Update of the Interpretations of Financial and Operational Rules)**
    - *Regulatory Notice* 23-21 (FINRA Reminds Member Firms of Net Capital, Recordkeeping and Financial Reporting Requirements in Connection with Revenue Recognition Practices)
    - *Notice to Members* 03-63 (SEC Issues Guidance on the Recording of Expenses and Liabilities by Broker/Dealers)
- SEC
  - Frequently Asked Questions Concerning the Amendments to Certain Broker-Dealer Financial Responsibility Rules
  - **SEC No-Action Letter Re: Broker-Dealer Capital Charges in Connection with the Creation and Redemption of SEC-Registered Exchange-Traded Funds**
- FASB
  - **606 Revenue from Contracts with Customers**
- SIFMA
  - **Syndicate Communication: Open Contractual Commitment**

## LIQUIDITY RISK MANAGEMENT

### Regulatory Obligations

**SEA Rule 15c3-3 requires firms to segregate customer assets and maintain reserve accounts, which constrains firms' available liquidity and necessitates careful planning to meet both customer protection requirements and operational funding needs. Additionally, SEA Rule 15c3-1 (Net Capital Rule) establishes minimum capital requirements that directly impact firms' liquidity positions and funding flexibility.**

**FINRA continues to emphasize effective liquidity and funding risk management as an important component of broker-dealers' financial responsibility. This is reflected in several *Regulatory Notices*, including *Regulatory Notice* 10-57 (Funding and Liquidity Risk Management Practices),** *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). These *Notices* emphasize the importance of maintaining adequate liquidity buffers, stress testing and contingency funding plans.

FINRA's Supplemental Liquidity Schedule (SLS)[37] **is designed to improve FINRA's ability to monitor for events that signal an adverse change in liquidity risk of firms with significant customer and counterparty exposures.**

### FINRA has noted instances where firms have reported inaccurate or incomplete information on the SLS. Examples include:

- incorrectly reporting agent lenders rather than underlying principals as counterparties to securities borrowed transactions, and/or failing to report the clearing organization as the counterparty to repurchase and reverse repurchase agreements for contracts novated to that clearing organization;
- providing incomplete information regarding noncash securities lending transactions (*i.e.*, identifying either the received collateral or delivered collateral, but not both) and within the Clearing deposit section (*e.g.*, missing dates, including weekends in the Largest Single Intramonth Amount Deposited Line Items, reporting month-end deposits instead of the actual Largest Single Intramonth Deposits); and
- not completing the line item for "Total Available Collateral in Broker-Dealer's Custody" (or entering inaccurate information).

### Impact Assessment: Daily Reserve Formula Computations

The SEC extended the compliance date for the amendments to Rule 15c3-3(e)(3)(i)(B)(1), which require certain firms exceeding a specified threshold to increase the frequency of their reserve formula computations from weekly to daily, to June 30, 2026.

- The increased frequency of computations and timing of resulting deposits and withdrawals may have a material impact on funding and liquidity.
- Firms should consider how these changes will affect their funding needs, stress tests, and contingency funding plans.
- For additional information, please see the SEC's Daily Computation of Customer and Broker-Dealer Reserve Requirements under the Broker-Dealer Customer Protection Rule and the Recent SEC Rule Amendments and Guidance Concerning Rule 15c3-3 "callout" box in the Protection of Customer Assets topic.

## Effective Practices

- *Liquidity Risk Management Updates:* Updating liquidity risk management practices, policies and procedures to conform with the firm's current business activities, including:
  - establishing governance for liquidity risk management, including determining who is responsible for monitoring the firm's liquidity position, the frequency of monitoring, and the communication and coordination protocols; and
  - creating a liquidity management plan that considers:
    - liquidity use assumptions that are based on both idiosyncratic and market-wide conditions and stress scenarios;

- sources of funding in both business-as-usual and stressed conditions;
- stability and other characteristics of funding sources (*e.g.*, restrictive covenants or material adverse change clauses within funding contracts that could affect the availability of the funding under certain conditions);
- the type and quantity of available collateral needed to secure funding;
- potential mismatches in duration between liquidity sources and uses;
- a contingency plan, in the event of loss of funding sources, that would provide sources of liquidity for operating under idiosyncratic market or 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 funding would be used; and
- early warning indicators of liquidity loss and escalation procedures.

- *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 the firm's historical data;
  - the firm's sources and uses of liquidity;
  - changes to the stability and quality of liquidity sources relied upon for its funding needs in a stressed environment;
  - material swings in customer cash balances (*e.g.*, redemptions, interest payments, sweeps);
  - the potential impact of off-balance sheet items (*e.g.*, nonregular way settlement trades, forward contracts and related margin requirements) on the firm's liquidity needs;
  - substantial regulatory or product changes;
  - **a robust data governance framework to enable accuracy, completeness, timeliness, and consistency of stress test and source data**; and
  - periodic governance review of stress test parameters based on current data.
- *Contingency Funding:* Considering any restrictive covenants and material adverse change clauses in contracts that could impact the availability of contingency funding.

## Additional Resources

- FINRA
  - Funding and Liquidity Key Topics Page
  - Frequently Asked Questions: Supplemental Liquidity Schedule
  - *Regulatory Notice* 23-11 (FINRA Seeks Comment on Concept Proposal for a Liquidity Risk Management Rule)
- SEC
  - Daily Computation of Customer and Broker-Dealer Reserve Requirements under the Broker-Dealer Customer Protection Rule (Dec. 20, 2024)

# PROTECTION OF CUSTOMER ASSETS

## Regulatory Obligations

SEA 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 customers' fully paid and excess margin securities and safeguard customer funds.

Firms satisfy these requirements by keeping reserves in a special reserve bank account and by maintaining customer securities in their physical possession or in a good control location, as specified in Rule 15c3-3. Firms are required to maintain a reserve of cash or qualified securities in the special reserve bank account that is at least equal in value to the net cash owed to customers.

### Recent SEC Rule Amendments and Guidance Concerning Rule 15c3-3

- The SEC extended the compliance date for the amendments to Rule 15c3-3(e)(3)(i)(B)(1), which require firms exceeding a specified threshold to increase the frequency of their reserve formula computations from weekly to daily, to June 30, 2026.
  - The SEC's amendments to Rule 15c3-3 and Rule 15c3-1, permitting broker-dealers that perform a daily customer reserve computation to decrease customer-related receivables, or "aggregate debit items," by 2 percent rather than 3 percent in the computation, was not impacted by the above noted extension.
  - Firms using the alternative net capital method can still choose to perform daily reserve computations and take the 2 percent debit reduction by notifying their DEA 30 days prior.
  - For additional information, please see the SEC's Daily Computation of Customer and Broker-Dealer Reserve Requirements under the Broker-Dealer Customer Protection Rule.
- The SEC amended Rule 15c3-3a to permit margin required and on deposit at covered clearing agencies providing central counterparty services for U.S. Treasury securities resulting from a customer's U.S. Treasury securities activity to be included by broker-dealers as a debit in the customer and proprietary accounts of broker-dealers reserve formulas, subject to certain conditions.
  - For additional guidance, please see the SEC's Division of Trading and Markets: Frequently Asked Questions – Treasury Clearing and Rule 15c3-3a.
- The SEC's Division of Trading and Markets staff published FAQs relating to crypto asset activities and distributed ledger technology, and withdrew the 2019 Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities.
  - The FAQs address possession or control requirements for crypto asset securities, clarifies that paragraph (b) of Rule 15c3-3 does not apply to crypto assets that are not securities, and provides guidance regarding control locations for compliance with paragraph (c) of the rule.

## Findings

- *Inadequate Supervision:* Failing to establish and maintain a reasonably designed supervisory system for **determining the required reserve deposit**, resulting in issues including:
  - incorrectly designating customer accounts as noncustomer accounts for purposes of the reserve formula computation; and
  - failing to identify, track or age suspense items.
- ***Treatment of Free Credit Balances – Transfers to Another Account or Institution:***
  - **Failing to obtain appropriate specific authorization prior to transferring customer funds to a third party.**
  - **Failing to transfer those funds as specified in such authorization.**
- *Inaccurate Reserve Formula Computations:* Failing to complete accurate reserve formula computations due to factors including:
  - inadequate supervisory procedures and processes; and
  - limited coordination between various internal departments.
- *Insufficient Segregation of Customer Securities:* Failing to maintain possession or control of customer fully paid or excess margin securities due to inadequate supervisory procedures and processes to identify, monitor and resolve possession or control deficits, and inaccurate coding of good control locations.
- **Failing to grant adequate access to FINOPs (particularly those who are part-time or contracted) to appropriate books and records to fulfill required duties.**
- **Failing to adequately complete reconciliations with external parties to confirm the firm's books and records reflect proper ownership and location of customer assets.**

### FINRA Reminds Firms of Their Obligation to Designate FINOPs

- For more information regarding a member firm's obligations related to the designation of FINOPs and FINOP duties, please see the 2025 FINRA Annual Regulatory Oversight Report, Segregation of Assets and Customer Protection – FINRA Reminds Firms of Their Obligations to Designate FINOPs callout box.

## Effective Practices

- *Periodic Evaluation of the Reserve Formula Computation Process:* Performing variance analysis to review for material fluctuations, anomalies and new items to identify potential inaccuracies; establishing a process to identify system or operational changes that could impact the customer or PAB reserve formula computations; and reviewing adjustments to the reserve formula computations to ensure they are accurate and compliant with the Customer Protection Rule.

- *Good Control Locations:* Ensure that all relevant documents are maintained to support the treatment of accounts as good control locations and perform periodic reviews to identify newly established accounts, potential miscoding, out-of-date paperwork or inactivity.
- *Check Forwarding Blotter Review:* Creating and reviewing the firm's checks received and forwarded blotters to confirm that they are accurately maintained and include the information required to evidence compliance with the Customer Protection Rule exemption (Rule 15c3-3(k)(2)(ii)).
- *Supervision:* Ensuring experienced individuals perform and supervise reserve formula computations and possession or control processes (who also hold the proper registrations).

## Additional Resources

- FINRA
  - Interpretations to the SEC's Financial and Operational Rules
- SEC
  - **Standards for Covered Clearing Agencies for U.S. Treasury Securities and Application of the Broker-Dealer Customer Protection Rule with Respect to U.S. Treasury Securities (Feb. 25, 2025)**
  - Daily Computation of Customer and Broker-Dealer Reserve Requirements under the Broker-Dealer Customer Protection Rule (Dec. 20, 2024)
  - **Frequently Asked Questions Concerning the Amendments to Certain Broker-Dealer Financial Responsibility Rules (July 1, 2020)**

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

Firms have shared the following ways they have used prior FINRA publications, such as Exam Findings Reports, Priorities Letters and Reports on FINRA's Examination and Risk Monitoring Program, to enhance their compliance programs. Firms may consider these practices, if relevant to their business model. We welcome feedback on how our firms use FINRA publications.

- *Assessment of Applicability:* Performed a comprehensive review of the findings 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 noted in Priorities Letters and the effective practices in Exam Findings Reports, and determined whether their compliance programs have any gaps that could lead to the types of findings noted in Exam Findings 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 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, and effective practices from our reports, as well as additional guidance from firms' policies and procedures to their Firm Element and other firm training.

## Endnotes

1 17 CFR 248.30(a)(1).

2 *See* 17 CFR 248.201(b)(3), which defines "covered account" as: (i) an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties; and (ii) any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

3 17 CFR 248.201(d).

4 The term "phishing" refers to fraudulent schemes in which scammers send electronic communications purporting to be from a trustworthy entity or individual, and attempt to trick the recipient to reveal PII through certain actions (*e.g.*, clicking on a link, opening an attachment). *See* Industry Risks and Threats – Resources for Member Firms for examples of prior phishing campaigns that targeted firms.

5 The term "smishing" refers to fraudulent schemes in which scammers send text messages designed to manipulate targets into taking an unsafe action (*e.g.*, clicking a link, replying with sensitive information). *See* the *Investor Insights* article Avoid Fraud: Be Alert to Investor Risks from SMS Phishing Scams for additional guidance related to identifying, preventing and responding to these schemes.

6 The term "quishing" refers to business email compromise attacks that uses QR codes in embedded PDFs to redirect victims to phishing URLs. *See* FINRA Cyber Alert—ONNX Store Purportedly Targeting Firms in Quishing Attacks for additional guidance related to identifying and preventing these attacks.

7 31 U.S. Code § 5311(1).

8 Capital Acquisition Broker (CAB) Rule 331 (Anti-Money Laundering Compliance Program) applies AML compliance program requirements to Capital Acquisition Brokers.

9 **For effective practices related to external fraud threats, *see Regulatory Notice* *22-21* (FINRA Alerts Firms to Recent Trend in Fraudulent Transfers of Accounts Through ACATS), the *Investor Insights* article Avoid Fraud: Protecting Your Investment Accounts From GenAI Fraud and FINRA's Firm Checklist for Compromised Accounts.**

10 **For additional guidance related to identifying and avoiding potential disaster-related scams, *see* the *Investor Insights* article Avoid Fraud—Beware of Stock Fraud in the Wake of Natural Disasters.**

11 **For additional guidance, *see* the *Investor Insights* article Avoid Fraud—Avoiding Pump-and-Dump Scams.**

12 **For additional guidance on identifying and avoiding both relationship investment scams and crypto investment scams, *see* the *Investor Insights* article Avoid Fraud—Relationship Investment Scams: What They Are and Tips to Avoid Them and the infographic *Crypto Investment Scams*.**

13 ***See* the Senior Investors and Trusted Contact Persons topic for additional guidance.**

14 ***Id.***

15 *See* Increase in Small Cap Fraud Involving Exchange-Listed Equities "callout" box in the Manipulative Trading topic for additional guidance.

16 **For additional guidance, *see* the Federal banking agencies' *Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations*.**

17 **For additional guidance, *see* the SEC Identity Theft Red Flags Rule Template and *Regulatory Notice* 19-18 (FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations).**

18 An identity verification method where applicants upload a photo or video of themselves, which is then compared with their recently submitted identity documents. (*See Regulatory Notice* 21-18 (FINRA Shares Practices Firms Use to Protect Customers from Online Account Takeover Attempts).)

19 *See Regulatory Notice* 22-25 (Heightened Threat of Fraud).

20 Key systems can involve areas such as trading systems; clearing, carrying, and settlement functions; cybersecurity; and technology services. However, the use of these systems may vary at individual broker-dealers, depending on their business model or reliance on the use of technology within their business operations. Key systems may also be used to support covered functions (as defined by FINRA Rule 1220 (b)(3)(A)(ii) (Customer Account Statements)).

21 *See* the Report's GenAI: Continuing and Emerging Trends topic for additional guidance.

22 *See* the Report's GenAI: Continuing and Emerging Trends topic for additional guidance.

23 In the context of the Report, "Off-Channel Communications" are defined as business-related communications sent or received on a communication tool that has not been authorized for business use. Off-Channel Communications can include, but is not limited to, electronic messaging services such as instant messaging applications, text messages, personal email, direct messaging applications, chat services, and messaging features through third-party vendor applications or social media platforms that are not routinely captured, supervised or retained by an associated person's member firm systems.

24 *See* FINRA Provides Update on Member Firms' Crypto Asset Activities.

25 *See* the Report's Private Placements topic for additional guidance related to conducting reasonable due diligence on unregistered offerings.

26 *See* the Report's GenAI: Continuing and Emerging Trends topic for additional guidance.

27 For additional context, *see* FINRA *Regulatory Notice* 23-08 (FINRA Reminds Members of Their Obligations When Selling Private Placements) noting particular concern where the firm or its associated persons are affiliated with the issuer or when red flags are present.*See also* the Report's Private Placements topic for additional findings related to firms and their associated persons recommending private offerings without having a reasonable basis.

28 *See* the Report's Annuities Securities Products topic for additional findings related to firms not reasonably supervising variable annuities or RILA recommendations for compliance with Reg BI.

29 *See* the Report's Annuities Securities Products topic for additional findings concerning failure to comply with Reg BI's Conflicts of Interest Obligation.

30 *See* the Report's Reg BI and Form CRS topic for additional information concerning Reg BI.

31 Interim value risk refers to the potential variability in the annuity's value if an investor decides to access account value before the end of the segment term. RILAs typically assess gains or losses based on the performance of a chosen market index over a set period. Accessing account value prior to the end of this period necessitates an interim valuation, based on a calculation separate from index performance, which therefore may not align with the initial expectations of the contract holder and which may result in significant loss.

32 The CAIS Amendment was proposed on March 13, 2025, and amended on May 28, 2025. *See* Securities Exchange Act Release No. 102665 (Mar. 13, 2025), 90 FR 12845 (Mar. 19, 2025) (Notice of Filing of Amendment to the National Market System Plan Governing the Consolidated Audit Trail); and Letter from Brandon Becker, CAT NMS Plan Operating Committee Chair, dated May 28, 2025 ("CAIS Amendment").

33 *See Regulatory Notice 20-31* (FINRA Reminds Firms of Their Supervisory Responsibilities Relating to CAT).

34 In this situation, the routing firm and receiving firm may have different best execution obligations. *See* Supplementary Material .09 to FINRA Rule 5310 (Best Execution and Interpositioning).

35 *See* Division of Market Regulation, Staff Legal Bulletin No. 13A, Frequently Asked Questions About Rule 11Ac1-6, FAQ #9.

36 ***See* the Report's Manipulative Trading topic for additional guidance.**

37 ***See Regulatory Notice 21-31* (FINRA Establishes New Supplemental Liquidity Schedule (SLS)).**

H39031—11/25