FINRA's 2025 Annual Regulatory Oversight Report: Focus on AI, Other Emerging Risk Areas, and Best Practices

FEBRUARY 18, 2025

By Stephanie Nicolas, Elizabeth L. Mitchell, Michael J. Leotta, Andre E. Owens, Susan Schroeder, Ayana Dow and Joshua Nathanson

On January 28, 2025, FINRA published its Annual Regulatory Oversight Report (the Report).[1] The Report highlights emerging risk areas and recent developments, common compliance deficiencies, and best practices for member firms. The Report is important not only because it identifies areas where FINRA is likely to be focused over the coming months but also because it provides insight into FINRA's expectations for the types of controls, procedures, and supervisory frameworks that firms should have in place to address priority risk areas and activities. This year, the Report highlights new considerations relating to the use of artificial intelligence (AI), which implicate multiple regulatory areas and activities – including third-party vendors and outsourcing, cybersecurity, communications with the public, and Regulation Best Interest.

In this Alert, we do not cover every topic addressed in the Report, but rather discuss the more notable additions to the Report for 2025 and our key takeaways, which we divide into the following topics: (1) the use of AI tools and technology, (2) the use of third-party vendors, (3) financial crimes prevention (cybersecurity, AML, and manipulation), (4) sales and trading, and (5) back-office and operations (including recordkeeping). By leveraging the insights highlighted in these areas and the Report more generally, firms can mitigate their regulatory risk and better position themselves for 2025.

1. *Artificial Intelligence*

[1] 2025 FINRA Annual Regulatory Oversight Report (January 2025), *available at* https://www.finra.org/sites/default/files/2025-01/2025-annual-regulatory-oversight-report.pdf.

The Report reflects FINRA's continued and enhanced focus on AI, in particular generative AI ("Gen AI").[2] Labeling AI a "continuing and emerging trend," the Report highlights FINRA's efforts to stay current on the evolving AI landscape and its impact on the industry and invites continued engagement from the industry. At the same time, the Report emphasizes that FINRA's rules are technology neutral and apply to AI as they apply to any other technology or tool. To the extent firms find ambiguity in the application of FINRA rules based on their specific Gen AI use cases, the Report encourages firms to seek interpretive guidance and to engage with their FINRA Risk Monitoring Analyst.

Leveraging FINRA's observations to date, the Report highlights specific considerations for firms that use or are contemplating the use of Gen AI tools.

- Enterprise-level supervision: Firms should focus on supervision of AI at an enterprise level, as well as by individual associated persons.
- Accuracy/bias risk mitigation: Firms should consider how to identify and mitigate risks of inaccuracy or bias in the use of Gen AI tools.
- Third-party vendor-driven AI: Firms using foundation AI models provided by third parties and third-party vendors that include Gen AI within their existing solutions must continue to ensure compliance with applicable regulatory requirements.
- Cybersecurity program design: A firm's cybersecurity program should consider:
    - risks associated with the firm's and third-party vendor's use of AI, such as leakage of customer PII and proprietary information of the firm based on prompts entered by employees, and
    - risks associated with a threat actor's potential exploitation of AI to attack the firm and its customers.

Related to this last point, the Report contains a callout box focused on what it terms the "adversarial use" of Gen AI by bad actors, including Gen AI–enabled fraud. This discussion highlights examples of how bad actors' use of Gen AI can amplify threats to investors, firms, and the securities markets, such as via ransomware attacks, the compromise of business emails to trick firm employees into conducting fraudulent transfers, imposter scams that lure victims into investing with fraudulent entities, and market manipulation by spreading false information on social media. The Report suggests that firms consider communicating with their employees and customers about such threats and steps they can take to mitigate them.

A more detailed discussion of the Report's focus on AI-related considerations with regard to third-party vendors, AML programs, and communications with clients is below.

[2] The Report defines "generative artificial intelligence" as "a type of artificial intelligence that, based on a user's prompt, can create content such as text, computer code, audio and video." *See* Report, at n.1.

2. *Third-Party Risk Landscape*

The Report highlights third-party risk (outsourcing) as a new area of regulatory focus for 2025.[3] In particular, it notes that FINRA has observed an increase in reliance on third-party vendors by firms to fulfill both regulated and non-regulated functions. At the same time, there has been an increase in the number of cyberattacks and outages at these providers. FINRA is concerned that a cyberattack or an outage at a third-party vendor could impact a large number of firms. Notably, the Report highlights a number of effective practices for managing third-party risk, including the following:

- Due diligence: Firms should have reasonably tailored initial and ongoing due diligence on third-party vendors that support systems related to key areas (*e.g.*, information technology and cybersecurity, AML monitoring). These processes should include:
  - validating data protection controls in third-party vendor contracts;
  - addressing third-party vendors' use of vendors (*i.e.,* fourth-party vendors) that may handle firm data;
  - asking potential third-party vendors if they incorporate Gen AI into their products or services and, if they do, evaluating the regulatory impact and response (*e.g.*, whether vendors should be prohibited from ingesting firm or customer sensitive information into their Gen AI tool);
  - reviewing, and as appropriate adjusting, third-party vendor tool default features and settings to comply with applicable regulatory obligations (*e.g.*, disabling a chat feature that may not be captured for supervisory review);
  - assessing third-party vendors' ability to protect sensitive firm and customer nonpublic information and data;
  - asking third-party vendors if they use foundation models provided by third-party vendors; and
  - establishing supervisory controls for a third-party technology vendor's business impact, including assessments and contingency plans.
- Creating an inventory: Firms should maintain a list of all third-party services (including hardware and software components provided by third parties) that the firm's technology infrastructure uses. This inventory can, among other things, help firms assess the impact of a cybersecurity incident or technology outage at a third-party vendor.

---

[3] The SEC 2025 exam priorities are similarly focused on outsourcing arrangements. SEC Fiscal Year 2025 Examination Priorities (Oct. 21, 2024), *available at* https://www.sec.gov/files/2025-exam-priorities.pdf (SEC 2025 Exam Priorities). In considering their outsourcing programs and related supervisory processes, broker-dealers should consider the guidance in the Report and in NASD Notice to Members 05-48 and FINRA Regulatory Notice 21-29, which establish a general framework for broker-dealer outsourcing arrangements. In addition to the considerations discussed in the Report, this earlier guidance discusses associated person and licensing considerations for third-party vendors.

- Offboarding: Firms should develop procedures that address offboarding vendors, including (1) the return or destruction of firm data at the termination of a third-party vendor contract, and (2) revoking a third-party vendor's access to systems, data, and corporate infrastructure when the relationship ends.
- Escalation protocol: Firms should have a formal process for evaluating the impact on the firm's ability to meet its regulatory obligations if the third-party vendor fails to perform the outsourced activity or function, and escalating as appropriate.

The Report also emphasizes the importance of proper due diligence for outsourcing arrangements where the arrangement is intended to satisfy a specific regulatory obligation. To this end, the Report contains outsourcing observations relating to compliance with Regulation S-P, CAT compliance, Rule 606 reports, OTC quotations, AML/CIP programs, and determining the correct price for fixed-income securities.

3. *Financial Crimes Prevention (Cybersecurity and Fraud, Market Manipulation, and AML)*

Cybersecurity and Fraud

The Report identifies new types of cyber fraud that appear to be on the rise, including account fraud, account takeovers, data breaches, imposter sites, quishing (*i.e.*, compromise attacks that use QR codes to redirect victims to phishing URLs), quasi-advanced persistent threats (APTs),[4] Gen AI–enabled fraud, and cybercrime-as-a-service. To address these risks, FINRA identifies the following new recommended practices:

- regularly conducting a "tabletop exercise" to bring key internal and external stakeholders together and ensure current and emerging cyber and technology threats and risks are appropriately identified, mitigated, and managed;
- subdividing networks into separate sections (*i.e.*, segment networks) to restrict the ability of threat actors to move across networks to find valuable data; and
- considering whether the firm's cybersecurity program addresses risks associated with threat actors' potential exploitation of Gen AI to increase the number, credibility, or severity of attacks (*e.g.*, fake web personas, deepfake audio and video, creation of advanced malware and other malicious tools).

Manipulative Trading

[4] FINRA defines quasi-APTs as "well-resourced threat actors that engage in sophisticated, malicious cyber activity targeted and aimed at prolonged network or system intrusion (*i.e.*, APTs), but are not necessarily sponsored by nation states or large organizations." Report, at p. 4.

The Report identifies manipulative trading in small-cap IPOs as a new risk area, noting that in 2024 these schemes evolved to include manipulative trading of shares originating from apparent nominee accounts that invest in small-cap IPOs and then funnel these shares to foreign omnibus accounts that liquidate them for profit. To help firms address these risks, the Report identifies several new effective practices:

- tailoring supervisory systems and processes to differing 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 (1) customer accounts (foreign or domestic) referred by a microcap issuer to the underwriting broker-dealer (particularly when the same officer or CEO has been noted across multiple issuers) and (2) money movements between the issuer and customer accounts; and
- monitoring for red flags indicating (1) conflicts of interest in private capital raises in advance of IPOs (particularly where a nominee controls shares), and (2) the involvement and participation in underwriting and selling activities by unregistered individuals in private and public offerings.

In a separate section on cryptocurrency, the Report includes a new discussion of crypto asset–related market abuse by bad actors that are taking advantage of investor interest in crypto and engaging in manipulative schemes similar to those in the equities market that are commonly associated with low-priced securities (e.g., pump-and-dump schemes). The Report does not provide more detail on effective practices but refers to prior guidance on, among other things, red flags involving low-priced securities.[5]

Anti-Money Laundering

In the AML section, the Report includes new observations relating to the use of Gen AI by bad actors, including:

- new account fraud and account takeovers: creating synthetic IDs, deepfake media, and malware to establish new fraudulent brokerage accounts or take over a customer's brokerage account;
- business email compromise: using Gen AI–enhanced social-engineering schemes to compromise firm email accounts (*e.g.*, tailoring the text in phishing emails to appear to be written for each individual target);
- ransomware attacks: conducting phishing campaigns with Gen AI–enhanced digital media (*e.g.,* fake emails, text, and phone and video calls that appear realistic) and using Gen AI–enhanced malware; and

[5] *See* FINRA Regulatory Notice 21-03.

- market manipulation: using Gen AI–created images or deepfake videos to spread false information on social media to move a company's stock price.

At the same time, the Report highlights a number of new effective practices for firms to combat these new risks:

- unusual withdrawal requests: firms should conduct thorough inquiries when customers (particularly those who may be elderly or vulnerable) request that an unusually significant amount of funds be disbursed to a personal bank account;
- reviewing clearing firm transactions: firms should review clearing firm transactions on a firm-by-firm basis to identify patterns of potentially suspicious transactions.[6]
- for firms that engage in low-priced securities or small-capitalization IPOs: firms should ensure that their reasonably designed AML procedures detect and respond to red flags associated with that activity; and
- regularly testing controls: firms should regularly review alerts or exception reports to ensure they are functioning as intended and that the firm's surveillance systems properly ingest the required data.

4. *Sales and Trading*

Communications with Clients – Use of AI

The Report includes a number of new findings and observations relating to firms' communications with clients, including the use of communications where Gen AI was used to create or assist in the creation of the communications. In particular, the Report reminds firms that:

- when using Gen AI technology to create or otherwise assist in creating communications to customers, these communications should be reviewed for compliance with federal securities laws and regulations and FINRA rules;
- where chatbot communications are used with investors, firms should ensure appropriate supervision of those communications and retention of those chat sessions in accordance with SEC and FINRA rules; and
- retail communications that mention AI tools, AI services (*e.g.*, portfolio construction, research) or products that rely on AI management should accurately describe how these

[6] Related to clearing, the Report also identifies new areas of suspicious and fraudulent activity related to automated clearing house (ACH) fraud, which consists of two types of fraud: (1) first-party ACH fraud (where a customer initiates a fraudulent ACH reclaim without sufficient funds); and (2) third-party ACH fraud (where a bad actor conducts a fraudulent ACH transaction by using stolen or synthetic information). According to FinCEN, ACH fraud was the most reported suspicious activity in securities and futures SAR filings between 2014 and 2022. Also, on October 1, 2024, the National Automated Clearinghouse Association issued new requirements that all non-consumer participants in the ACH network implement fraud detection and monitoring programs.

offerings incorporate AI technology and balance the discussion of benefits with appropriate discussion of risks.

Regulation Best Interest

The Report repeats prior SEC and FINRA guidance on Regulation Best Interest (Reg BI). Most of the Report's new findings relate to the Care Obligation and Conflict of Interest Obligation. In particular, with regard to the Care Obligation, the Report contains the following new reminders:

- For offerings (in particular, private placements), the Report reminds firms and their associated persons not to rely "solely on information from the issuer or its affiliate" in their investigation of securities offerings.
- With regard to risky or complex products, the Report reminds firms to develop a sufficient understanding of the features and risks of a recommended security or investment strategy involving a security and specifically notes that broker-dealers should understand holding-period risk associated with leveraged and inverse exchange-traded products and bondholders' rights with respect to high-risk bonds. Separately, FINRA is focused on whether broker-dealers and their associated persons are recommending complex or risky products that result in concentrations that are inconsistent with firm limits or the retail customer's risk tolerance or investment objectives.
- With regard to switching, the Report reminds firms and their associated persons that they should not recommend that a customer replace or switch existing products without understanding associated risks and costs, including surrender charges and tax consequences. Examples of in-scope product switches include variable annuities, mutual funds, and 529 plans.
- With regard to brokerage versus advisory accounts, the Report reminds firms and their associated persons that they should compare the relevant costs and fees when determining whether to book trades in a customer's brokerage or advisory account or to recommend transfers of securities from one account to another. Note that SEC examinations staff also included in their 2025 exam "account allocation practices (*e.g.*, allocation of investments where an investor has more than one type of account) and account selection practices."[7]

For the Conflict of Interest Obligation, the Report notes deficiencies relating to 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. The Report provides, as an example, not disclosing an associated person's financial incentive to recommend the opening of new investment accounts at the firm's affiliate or to recommend bonds issued by a company in

[7] SEC 2025 Exam Priorities, at p. 8.

which the associated person had a significant personal ownership stake, the value of which largely depended on the bond sales.

While the Reg BI section does not address AI specifically, the Report does suggest, as a new effective practice, that firms ensure that any technology used to generate recommendations is coded to consider costs on both affiliated and non-affiliated investment products offered by the firm.

Annuities Securities Products

FINRA added a new section that specifically addresses annuities securities products, including registered index-linked annuities (RILAs). With an RILA, an investor's returns are based at least in part on the performance of an index or other benchmark over a set period. FINRA notes that the market for RILAs has grown significantly in recent years. The Report provides guidance on potential risks and costs associated with RILAs and other annuities securities products.

Form CRS and DBAs

Exchange Act Rule 17a-14 requires broker-dealers to publish a customer relationship summary (Form CRS) "prominently" on their website. The Report notes, as a new finding, failure to post Form CRS on a DBA website for retail broker-dealers that have registered representatives that do business under another name (i.e., a DBA name). There is more guidance on DBA websites and Form CRS in frequently asked questions posted on sec.gov.[8]

Extended Hours Trading

FINRA added a new section to the Report on extended hours trading. Retail investors have increasingly expressed a desire to trade outside of regular trading hours (*i.e.*, 9:30 a.m. to 4:00 p.m. ET). The Report notes that, in considering extended hours trading, firms should have procedures to comply with disclosures (Rule 2265), best execution (Rule 5310), supervision (Rule 3110), and trade and CAT reporting. In addition, procedures should address operational readiness, customer support, and business continuity planning.

5. *Operations and Back Office*

Books and Records

[8] "Frequently Asked Questions on Form CRS," Securities and Exchange Commission (accessed on Feb. 14, 2025), *available at* https://www.sec.gov/rules-regulations/staff-guidance/trading-markets-frequently-asked-questions/frequently-asked-questions-form-crs.

The Report identifies new findings and observations relating to firms' retention of business-related electronic communications, especially those conducted through unauthorized channels. For example, the Report highlights, as new observations, instances where firms:

- failed to review electronic communications for indications of associated persons' potential use of off-channel communications;
- failed to preserve and review business-related text messages;
- relied on policies and procedures that were overly general and did not adequately specify (1) permitted and prohibited platforms, (2) methods to determine if registered representatives were engaging in business communications on unapproved platforms, and (3) corrective actions for registered representatives if they violate firm policy and engage in business communication using unapproved platforms;
- reviewed electronic communications without selecting adequate samples or using targeted key word searches;
- failed to review electronic communications in non-English languages in which the member conducts business.
- did not properly supervise third-party vendors that support firms' monitoring of their associated persons' electronic communications, resulting in firms not supervising or retaining communications; and
- did not detect that associated persons used personal email accounts and other off-channel platforms to communicate with customers when conducting firm business.

In terms of new effective practices, the Report states that firms should have procedures to monitor for indications that associated persons are using off-channel communications (*e.g.*, a decrease or cease in activity on certain previously used firm-approved communication channels or tools). In addition, firms should consider frequently revising key words used to surveil for associated persons' potential use of off-channel communications, and tailoring key word searches to their business models.

Covered Clearing Agencies and Treasury Securities

Given the systemic importance of Treasury securities, the Report contains a new discussion emphasizing the need for robust risk management and transparency in clearing and settlement processes. On December 13, 2023, the SEC adopted new rules to enhance risk management in the U.S. Treasury market by establishing standards for covered clearing agencies, including capital, margin, and operational risk requirements.[9] FINRA observed that some member firms have

[9] 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, 89 Fed. Reg. 2714 (Jan. 16, 2024), *available at* https://www.govinfo.gov/content/pkg/FR-2024-01-16/pdf/2023-27860.pdf.

inadequately accounted for substantial regulatory or product changes, such as the centralized clearing of Treasuries.[10]

Segregation of Assets

The Report contains new findings and observations relating to the segregation of customer assets and compliance with customer protection rules. FINRA observed several deficiencies in firm custody practices, including instances where firms failed to complete accurate reserve formula computations and employed insufficient supervisory procedures to identify and resolve deficits. FINRA urges firms to implement oversight mechanisms to ensure customer funds and securities remain separate from proprietary firm accounts. Further, firms should have clear documentation and governance policies regarding how customer assets are handled.

Contributors

Michael J. Leotta
PARTNER

michael.leotta@wilmerhale.com
+1 202 663 6526

Elizabeth L. Mitchell
PARTNER

elizabeth.mitchell@wilmerhale.com
+1 202 663 6426

Stephanie Nicolas
PARTNER

stephanie.nicolas@wilmerhale.com
+1 202 663 6825

Andre E. Owens
PARTNER

andre.owens@wilmerhale.com
+1 202 663 6350

[10] Report, at p. 69.

Susan Schroeder
PARTNER

susan.schroeder@wilmerhale.com
+1 212 230 8865

Ayana Dow
ASSOCIATE

ayana.dow@wilmerhale.com
+1 202 663 6296

Joshua Nathanson
ASSOCIATE

joshua.nathanson@wilmerhale.com
+1 202 663 6193