MAYER | BROWN

FEBRUARY 21, 2025

FINRA PUBLISHES 2025 ANNUAL REGULATORY OVERSIGHT REPORT

NEW TOPICS AND CONTENT HIGHLIGHT FINRA'S INCREASED FOCUS ON CYBERSECURITY, THIRD-PARTY RISK, ARTIFICIAL INTELLIGENCE, INVESTMENT FRAUD AND OTHER RISK AREAS

The Financial Industry Regulatory Authority, Inc. ("FINRA") published its 2025 FINRA Annual Regulatory Oversight Report (the "Report"), which builds on the structure and content of FINRA's prior reports for 2021-2024. This year, the Report adds new topics relating to the third-party risk landscape, registered index-linked annuities ("RILAs"), and extended hours trading. The Report also includes new content on various topics from last year's report, including cybersecurity, artificial intelligence ("AI") (including generative AI ("Gen AI")), investment and Automated Clearing House ("ACH") fraud, FINRA's Remote Inspections Pilot Program, Residential Supervisory Location ("RSL") designation under FINRA rules, and trade reporting enhancements for fractional share transactions. Finally, the Report highlights new findings and effective practices relating to a wide range of topics covered by FINRA in prior years.

CERTAIN AREAS OF FOCUS

- **Cybersecurity**. FINRA continues to observe an increase in the variety, frequency and sophistication of certain cybersecurity attacks and incidents/outages that represent threats to the financial industry. The Report identifies several emerging cybersecurity-related emerging threats that firms should closely monitor, including specific types of cybersecurity attacks (e.g., new account fraud, account takeovers, imposter sites and "quishing"), Gen AI-enabled fraud and quantum computing risks, as discussed further below.
- **Third-Party Risk Landscape**. In light of an observed increase in cyberattacks and outages at third-party vendors, FINRA highlights several areas when developing and enhancing third-party vendor risk management programs, including:
    - Conducting initial or ongoing due diligence on third-party vendors that support systems related to key areas, such as information technology, cybersecurity and anti-money laundering ("AML") monitoring;
    - Validating data protection controls in third-party vendor contracts;

- Involving third-party vendors that support key systems in the testing of incident response plans;
- Maintaining a list of all third-party services, or third-party provided hardware or software components, that the firm's technology infrastructure uses;
- Having procedures that address the return or destruction of firm data at the termination of a third-party vendor contract; and
- Addressing third-party vendors' use of vendors (i.e., fourth-party vendors) that may handle firm data.

FINRA identifies certain effective practices when assessing and managing the risks associated with third-party vendors during the lifecycle of the relationship, including *asking potential third-party vendors if they incorporate Gen AI into their products and services*, and, if so, evaluating contracts with the vendors and requesting that they be amended (as necessary) to comply with the firm's regulatory obligations (e.g., prohibit firm or customer sensitive information from being ingested into a third-party vendor's open-source Gen AI tool). Moreover, firms should review (and, as appropriate, adjusting) third-party vendor tools' default features and settings to meet the firm's business needs and regulatory obligations (e.g., disabling a chat feature). Finally, the Report cites to several helpful "additional resources," including FINRA's Cybersecurity Advisory: Increasing Cybersecurity Risks at Third-Party Providers in September 2024. See our Legal Update for details regarding FINRA's Cybersecurity Advisory.

- **AI – Continuing and Emerging Trends / Adversarial Use of Gen AI**. FINRA notes that firms are proceeding cautiously with their use of Gen AI technology. In this regard, firms are generally exploring Gen AI tools to increase efficiency of internal functions, including with respect to information summarization, conducting analyses across disparate data sets, and retrieving relevant portions of policies or procedures. FINRA identifies several topics for firms to consider when contemplating the use of Gen AI technology, such as:
  - How to supervise the use of Gen AI on an enterprise level (as well as by individuals); and
  - How to identify and mitigate associated risks (e.g., accuracy, bias, leakage of firm or customer sensitive information).

  FINRA highlights that bad actors are increasingly exploiting Gen AI technology in ways that amplify threats to investors, firms and the securities industry, including through investment club scams, new account fraud and account takeovers and imposter scams, as discussed further below. Moreover, bad actors are using Gen AI technology to engage in market manipulation, such as by using Gen AI-created (realistic-looking or "deepfake") images or videos to spread false information on social media to move a company's stock price. FINRA encourages firms to consider whether their cybersecurity programs address 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 or other malicious tools).

- **Remote Inspections Pilot Program and RSL Designation**. The Report reminds firms of their obligations under FINRA Rules 3110.18 (Remote Inspections Pilot Program) and 3110.19 (Residential Supervisory Locations). See our Legal Update for details regarding the new rules. Additionally, as firms determine which offices/locations may be eligible for the RSL designation, they must satisfy their obligations to (i) identify their RSLs through Form U4 by answering the "RSL Question" therein and (ii) submit Form BR to register or close their branch offices (as applicable).

- **RILAs (Registered Index-Linked Annuities)**. FINRA treats RILAs as *complex financial products* and notes that the market for RILAs has grown significantly in recent years (more than quintupling since 2017, with annual RILA sales of $47.4 billion in 2023 alone). FINRA identifies deficiencies relating to firms' retail communications regarding RILAs, including: inadequately explaining how RILAs function; insufficiently explaining specialized terms specific to RILAs (e.g., cap rates, buffers); not including risk disclosures or disclosures regarding fees and changes; making exaggerated, misleading, unwarranted or promissory statements and claims (e.g., exaggerated use of the term "downside protection" in describing buffers); and making hypothetical illustrations that go beyond the sole purpose of showing how RILAs function. FINRA highlights as an effective practice applying heightened policies and procedures to recommendations of RILAs, such as the explicit requirements that apply to variable annuities under FINRA Rule 2330 (Members' Responsibilities Regarding Deferred Variable Annuities), including requiring a registered representative to document and sign his or her rationale for the recommendation, requiring a registered principal to review and determine whether he or she approves of the recommended purchase or exchange of a RILA (and to document and sign the basis of such approval), and implementing surveillance procedures to determine if any of the firm's representatives have rates of effecting RILA exchanges (or replacements of variable annuities with RILAs or vice versa) that may evidence conduct inconsistent with Reg BI. Please see also our Legal Update for additional information regarding the SEC's rule and form amendments concerning RILAs in July 2024.

- **Extended Hours Trading**. FINRA has observed a growing number of firms offering varying degrees of extended hours trading services (e.g., overnight period of 8 p.m. to 4 a.m. ET). FINRA reminds firms that participate in extended hours trading of their obligations to comply with FINRA and SEC rules applicable to such trading, including FINRA Rules 2265 (Extended Hours Trading Risk Disclosure), 5310 (Best Execution and Interpositioning) and 3110 (Supervision). FINRA also notes several effective practices relating to extended hours trading, such as (i) establishing and maintaining reasonably designed supervisory processes that address any unique characteristics or risks of such trading (e.g., order handling and volatile or illiquid market conditions) and (ii) evaluating unique operational readiness and customer support needs during overnight hours.

- **Upcoming Trade Reporting Enhancements for Fractional Share Transactions**. FINRA is planning to implement enhancements to the FINRA trade reporting facilities to support the reporting of fractional share quantities. The effective date of the enhancements will be announced in a future notice. Upon implementation of the enhancements, firms will be required to populate a new "Fractional Share Quantity" field by entering the entire quantity of the trade, including the fractional component up to six digits after the decimal. Notably, firms will continue to populate the existing "Quantity" field as they do today using whole numbers (with fractional amounts either rounded up or truncated).

SELECTED TOPICS

The Report addresses 24 regulatory topics organized into six sections: Financial Crimes Prevention; Firm Operations; Member Firms' Nexus to Crypto; Communications and Sales; Market Integrity; and Financial Management. We highlight below certain new topics for 2025 and new content that FINRA added to previously covered topics.

FINANCIAL CRIMES PREVENTION

The Financial Crimes Prevention section contains a significant amount of new content relating to: cybersecurity and cyber-enabled fraud; AML, fraud and sanctions; and manipulative trading.

FINRA has observed an increase in ***cybersecurity attacks*** and ***cyber-enabled fraud*** involving:

- *New account fraud*, in which threat actors use falsified customer information or stolen identity information to open accounts at financial institutions through a mobile app or internet browser;
- *Account takeovers*, where threat actors use compromised investor information (such as login credentials) to gain unauthorized access to online accounts;
- *Data breaches*, which involve threat actors accessing confidential firm and/or client information through an attack (and then exposing, or threaten to expose, this information to the clear or dark nets);
- *Imposter sites*, in which threat actors leverage sites, domains and social media profiles that impersonate financial firms, registered representatives and FINRA staff; and
- *Quishing*, which are compromise attacks that use QR codes to redirect victims to phishing URLs.

The Report highlights that ***third-party vendors*** can pose additional cyber threats to firms by introducing vulnerabilities that can lead to data breaches and supply chain attacks. Furthermore, the Report describes ***Gen AI-enabled fraud*** as an emerging threat that may impact firms. Gen AI-enabled fraud refers to scenarios in which threat actors exploit Gen AI's ease of use and wide range of applications to enhance their cyber-enabled crimes by, among other things, generating fake content such as imposter sites, false identification documents and deepfake audio and video. Finally, the Report identifies ***quantum computing*** as an emerging technology that could be exploited by threat actors to aggravate the risk of

cybersecurity-related crimes (particularly those with the ability to quickly break current encryption standards currently used in the financial services industry).

FINRA identifies an increase and evolution in ***investment fraud committed by bad actors who engage directly with investors***, typically by enticing victims to withdraw funds from their securities accounts and send the funds to the bad actors. FINRA lists several common types of investment fraud schemes:

- *Investment club scams*, in which bad actors post fraudulent social media advertisements (often using the likeness of well-known finance personalities unaffiliated with the scam) to direct victims to purported "investment clubs" on encrypted messaging applications, where victims are persuaded to purchase shares of low-volume and thinly traded securities;
- *Relationship investment scams*, whereby bad actors hide their true identities and reach out to unsuspecting targets (e.g., online, via text messages), gain the victim's trust over time, and then defraud them through fake investments;
- *Imposter websites* (described above); and
- *Tech support and support center scams*, in which bad actors impersonate a firm's customer support center through online sponsored advertising, with the goal to misdirect victims and steal their funds and/or personally identifiable information.

FINRA suggests several effective practices to help firms mitigate these threats, including monitoring for abrupt changes in customer behavior (e.g., a withdrawal request that does not align with the customer's typical behavior), educating firm personnel who are in direct contact with customers (e.g., how to recognize red flags, communicate with customers who may be victims, and escalate concerns), and 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 financial exploitation.

Additionally, FINRA identifies ***ACH fraud*** as a continuing risk, as FINRA has recently observed an increase in suspicious and fraudulent activity related to ACH transactions. FINRA describes several effective practices for mitigating vulnerabilities relating to ACH fraud, including: requiring additional identification and verification documents during account opening and initiation of ACH transfer requests (e.g., obtain customer account statements from the originating depository financial institution prior to processing an ACH transaction); contracting with third-party vendors that offer services to risk rank customers attempting to deposit funds in an account at a financial institution; and limiting the amount and number of outbound transfers from a brokerage account.

The Report contains new material related to ***manipulative trading***, including various observed surveillance deficiencies and effective practices. FINRA notes that it observed an evolution in manipulative trading schemes in small cap initial public offerings ("IPOs"), in which unusual price increases occurred in the weeks or months after certain small cap issuers' IPOs (rather than the day of or shortly after the IPOs, as typically observed in the past).

FIRM OPERATIONS

Third-Party Risk Landscape is a new topic in this section. This section also addresses: technology management; outside business activities and private securities transactions; books and records; senior investors and trusted contact persons; and crowdfunding offerings (broker-dealers and funding portals).

With respect to **technology management**, FINRA highlights the SEC's 2024 amendments to Regulation S-P, including firms' incident response programs and the requirement to provide customer notification in the case of unauthorized access or use of customer information. Larger entities must comply with the amendments by December 2, 2025, and smaller entities must comply with the amendments by June 3, 2026. See our Legal Update for details regarding the Regulation S-P amendments.

FINRA adds new content regarding **books and records requirements** under SEC Rules 17a-3 and 17a-4 and FINRA rules. FINRA identifies deficiencies relating to not retaining, archiving and reviewing non-email electronic communications conducted through firm-approved communication channels as well as not reviewing electronic communications for indications of associated persons' potential use of "off-channel communications" (i.e., business-related communications sent or received on a communication tool that has not been authorized by the firm for business use). FINRA also identifies deficiencies relating to policies and procedures that were overly general and did not adequately specify, for example, permitted vs. prohibited platforms, methods to detect associated persons' use of unapproved platforms for business communications, and corrective actions for associated persons violating firm policy regarding off-channel communications.

The Report sets forth effective practices relating to **senior investors and trusted contact persons**. Specifically, FINRA encourages firms to consider engaging in communication campaigns on fraud awareness, hosting educational webinars and providing customers with other resources to educate them on the latest scams. Additionally, firms should consider conducting training for both front- and back-office staff regarding common financial and investment scams and the warning signs of potential fraud or exploitation of customers as well as diminished capacity.

MEMBER FIRMS' NEXUS TO CRYPTO

FINRA reminds firms that the federal securities laws and FINRA rules apply to member firm activities involving crypto assets that are securities. Furthermore, certain FINRA rules apply to the activities of firms and their associated persons irrespective of whether the activity involves a security. The Report includes effective practices for firms when conducting due diligence of unregistered crypto assets that are securities, including understanding (i) the exemption from registration on which the unregistered offering will rely and (ii) token governance and ownership rights or allocations related to owning a token. The Report refers to certain additional resources relating to crypto assets, including FINRA's update on its Crypto Asset Targeted Exam in January 2024. See our blog post for details regarding this update.

COMMUNICATIONS AND SALES

The Communications and Sales section of the Report adds guidance relating to communications with the public, Reg BI and Form CRS, private placements, and variable annuities.

The Report contains new material relating to **communications with the public**, including with respect to the use of Gen AI technology, communications promoting securities lending programs, supervision of social media influencers, and retail communications focused on RILAs. Notably, FINRA observed the following effective practices relating to ***firms' use of Gen AI*** technology in their communications with the public: (i) reviewing Gen AI-generated communications to ensure they comply with applicable federal securities laws and regulations and FINRA rules; (ii) ensuring appropriate supervision, and retention, of Gen AI-generated (such as chatbot) communications used with investors; and (iii) ensuring that retail communications that mention AI tools, AI services, or products that rely on AI management accurately describe how they incorporate AI technology and balance the discussion of benefits with appropriate discussion of risks. With respect to ***securities lending programs***, firms should ensure that retail communications which promote or recommend income sharing programs to retail investors accurately and clearly disclose the terms and conditions of the program, including fees customers would receive. Lastly, FINRA notes deficiencies relating to firms' supervision of ***social media influencers' communications*** on behalf of such firms (e.g., not reviewing influencers' videos prior to posting on social media platforms; not retaining those videos).

With respect to **Reg BI** and **Form CRS**, the Report identifies several findings related to ***complex or higher-risk products***, such as making recommendations without developing a sufficient understanding of the features and risks of the recommended security or investment strategy involving a security, recommending complex or risky products that do not align with the retail customer's investment profile, and recommending 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 objectives. Additionally, with respect to failures to comply with the Conflict of Interest Obligation under Reg BI, FINRA's findings include 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., financial incentive to recommend the opening of new investment accounts at the firm's affiliate). Findings related to Form CRS include that firms failed to timely re-file *with an exhibit highlighting the changes* in the Central Registration Depository (i.e., within 30 days of the date when Form CRS became materially inaccurate).

FINRA highlights several findings relating **private placements**, including firms misapplying the filing exemptions under FINRA Rule 5123(b) (e.g., misunderstanding the scope of the accredited investor exemption under FINRA Rule 5123(b)(1)(J), which does not include accredited investors who are natural persons), incorrectly purporting to not make recommendations of private placements (and, as a result, not exercising reasonable diligence, care and skill in making such recommendations), and failing to comply with SEC Rules 10b-9 and 15c2-4 regarding contingency offerings, in particular when the contingency terms are amended during the offering (e.g., significantly reducing the minimum contingency amount).

FINRA notes as an effective practice providing targeted, in-depth training to representatives about the firms' policies, process and filing requirements prior to recommending an offering.

With respect to **annuities securities products**, the Report adds new findings and effective practices relating to RILAs (see discussion in Certain Areas of Focus above). Additionally, FINRA's findings include recommendations of variable annuity exchanges that were unsuitable for, or 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 an increase in expenses or fees to the customer or the loss of material benefits (e.g., loss of a living benefit rider). Firms should use disclosure forms to provide customers with meaningful information about the advantages and disadvantages of recommended exchanges.

MARKET INTEGRITY

The Market Integrity section of the Report discusses: the Consolidated Audit Trail ("CAT"); customer order handling – best execution and order routing disclosures; Regulation SHO – bona fide market making and close-out requirements; fixed income – fair pricing; OTC quotations in fixed income securities (SEC Rule 15c2-11); and the Market Access Rule (SEC 15c3-5). Extended hours trading is a new topic in this section (see discussion in Certain Areas of Focus above).

The Report includes new content on supervisory deficiencies relating to **CAT**, including not implementing an accuracy review (as described in FINRA Regulatory Notice 20-31), not using a reasonable sample size when selecting firm CAT reports for review, and not supervising reporting agents that report to CAT on the firm's behalf.

The Report also highlights **data integrity and timeliness issues in municipal underwriting filings**. Common issues include: not submitting Form G-32 data within the timeframes required by Rule G-32(b)(i)(A) of the Municipal Securities Rulemaking Board (the "MSRB"), submitting inaccurate data or submitting data in incorrect fields, omitting names of key stakeholders (e.g., syndicate members, municipal advisors), not correctly identifying advance refundings, and not correctly identifying limited offerings exempt from SEC Rule 15c2-12. FINRA highlights effective practices relating to reporting Form G-32 data, including requiring supervisory review of all Form G-32 data prior to submission, periodically reviewing prior data submissions to identify potential areas for improvement, and training personnel on Form G-32 submission requirements, timeframes, and terminology.

In respect of firms' **best execution** obligations, FINRA highlights firms' failure to establish written policies and procedures with respect to trading in securities with limited quotations or pricing information as set forth in Supplementary Material .06 of FINRA Rule 5310, including documenting compliance with such policies and procedures.

With respect to **order routing disclosures**, FINRA includes several effective practices for SEC Rule 606(a) reports, including that erroneous or rejected submissions to FINRA are corrected and resubmitted, hyperlinks in reports submitted to FINRA are operational, and reports made publicly available are consistent with the reports submitted to FINRA.

The Report specifies new findings relating to **fair pricing obligations for fixed income transactions**. For example, with respect to incorrect determinations of the "prevailing market price" (or "PMP") under FINRA Rule 2121 and MSRB Rule G-30, FINRA's findings include firms relying on third-party software to determine the PMP but not understanding how the software determines the PMP and/or ensuring that the software could access all information necessary to properly determine the PMP. Other findings include (i) permitting registered representatives to determine the PMP through manual overrides of the third-party software without appropriate supervision of, or maintaining documentation regarding, how the PMP was determined in manual overrides or (ii) determining PMP based on the firm's quotation prices rather than in accordance with the waterfall set forth in FINRA Rule 2121 or MSRB Rule G-30, as applicable.

With respect to **OTC quotations in fixed income securities**, FINRA reminds firms of the SEC's October 2023 order providing permanent exemptive relief for fixed income securities sold in compliance with the safe harbor set forth in Rule 144A under the Securities Act of 1933 and the SEC staff's November 2024 no-action letter to extend (without an expiration date) the relief previously provided for other fixed income securities. See our blog post for additional information.

Finally, FINRA highlights effective practices for compliance with the **Market Access Rule**: conducting training for individual traders regarding the steps and requirements for requesting *ad hoc* credit limits; reviewing any automated controls to timely revert *ad hoc* credit limit adjustments; and for firms that provide clients sponsored access, verifying the firm's ability to retain direct and exclusive control over pre-trade financial and regulatory requirements.

FINANCIAL MANAGEMENT

The Financial Management section of the Report discusses net capital, liquidity risk management, and segregation of assets and customer protection.

The Report highlights findings relating to **net capital**, including not having a reasonable process to determine when the firm has a net capital deficiency and should begin the process of suspending business operations, and ensure that it files timely notices of a net capital deficiency. Other findings include: filing notices that inaccurately reflected the firm's aggregate indebtedness, minimum required net capital or excess net capital; acting in the capacity as the lead underwriter without maintaining sufficient net capital to participate in the underwriting and cover the required open contractual commitments ("OCC") capital charges; and failing to accurately capture OCC charges on firm commitment offerings due to, for example, applying an incorrect haircut percentage on charges, only capturing charges for the day of the pricing date or the settlement date, and not capturing charges on the unsold portion of underwriting from pricing date through settlement date. FINRA reminds firms of the SEC's rule amendments in December 2024 to mandate certain filings and submissions under the Securities Exchange Act of 1934 to be made electronically and to make certain technical changes to the Financial and Operational Combined Uniform Single (FOCUS) Report. See our blog post for additional information regarding these amendments.

With respect to **liquidity risk management**, FINRA found instances of firms incorporating unreasonable assumptions into stress tests that materially misrepresent the firm's liquidity position, such as (i) inaccurately determining the amount of the firm's inventory that would require financing in a stressed environment and (ii) relying on funding sources in a stress event that the firm does not engage with in a business-as-usual environment. FINRA also notes that firm departments responsible for liquidity risk oversight (e.g., second and third lines of defense) did not identify unreasonable assumptions or inaccurate calculations that existed in liquidity stress tests.

The Free Writings & Perspectives, or FW&Ps, blog provides news and views on securities regulation and capital formation. The blog provides up-to-the-minute information regarding securities law developments, particularly those related to capital formation. FW&Ps also offers commentary regarding developments affecting private placements, mezzanine or "late stage" private placements, PIPE transactions, IPOs and the IPO market, new financial products and any other securities-related topics that pique our and our readers' interest. Our blog is available at: www.freewritings.law.

CONTACTS

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

STEFFEN HEMMERICH
+1 212 506 2129
SHEMMERICH@MAYERBROWN.COM

ANNA PINEDO
+1 212 506 2275
APINEDO@MAYERBROWN.COM

STEPHEN VOGT
+1 202 263 3364
SVOGT@MAYERBROWN.COM
