MAYER | BROWN

DECEMBER 18, 2025

FINRA PUBLISHES 2026 ANNUAL REGULATORY OVERSIGHT REPORT

THE REPORT HIGHLIGHTS FINRA'S CONTINUED FOCUS ON GENERATIVE ARTIFICIAL INTELLIGENCE, CYBERSECURITY, SMALL-CAP SECURITIES FRAUD, AND THIRD-PARTY RISK

The Financial Industry Regulatory Authority, Inc. ("FINRA") published its 2026 FINRA Annual Regulatory Oversight Report (the "Report"), which builds on the structure and content of FINRA's prior reports for 2021-2025. This year, the Report was published earlier than in prior years—aligning more closely with the Securities and Exchange Commission's ("SEC") release of its 2026 examination priorities.[1] The Report adds a new section on continuing and emerging trends in generative artificial intelligence ("GenAI"). It also includes new content on various topics, including cybersecurity and cyber-enabled fraud, manipulative trading in small-cap, exchange-listed equities, and the third-party risk landscape. In addition, the Report highlights new findings and effective practices relating to topics previously covered by FINRA. FINRA also uses the Report to highlight its FINRA Forward initiatives, which have as their objectives modernizing FINRA rules; empowering member firm compliance by enhancing FINRA's support for member firm compliance programs; and combatting risks related to cybersecurity and fraud by expanding FINRA's cybersecurity and fraud prevention activities.

CERTAIN FOCUS AREAS

- **GenAI – Continuing and Emerging Trends**. New for 2026, the Report dedicates a section to GenAI. FINRA has observed rapid GenAI adoption across the financial industry, with the most common GenAI use case among member firms being summarization and information extraction (*i.e.*, condensing large text and pulling out entities, relationships, and key facts from unstructured documents). Other use cases include: conversational AI and question answering (*e.g.*, chatbots, virtual assistants, and voice interfaces); translation (*e.g.*, convert audio to text or vice versa); content generation and drafting (*e.g.*, drafting documents, reports, marketing materials); and personalization and recommendation *(e.g.*, tailoring products, services, or content to customer preferences). FINRA cautions firms to consider how they will meet applicable regulatory obligations before testing and deploying GenAI, noting that FINRA's technologically neutral rules apply when firms use GenAI just as with any other technology or tool.
    - *Supervision and Governance*. FINRA highlights that firms should establish enterprise-level supervisory processes for developing and using GenAI, and adopt approaches to mitigate

risks relating to accuracy (*e.g.*, hallucinations) and bias. FINRA recommends firms implement a formal review and approval process involving business and technology experts to assess GenAI opportunities and requisite controls, including establishing a supervision, governance, or model risk management framework with clear policies and procedures to develop, deploy, use, and monitor GenAI while maintaining thorough documentation.

- *Cybersecurity*. Firms should also evaluate whether their cybersecurity program addresses risks from both their internal and third-party vendors' GenAI use, and whether tools, data provenance, and processes can detect threat actors' use of AI or GenAI against their systems.
- *Testing*. FINRA stresses that firms should conduct robust testing to understand model capabilities, limitations, and performance, including privacy, integrity, reliability, and accuracy checks.
- *Monitoring*. Firms should also continuously monitor prompts, responses, and outputs to ensure expected performance and compliance (*e.g.*, logging prompts and outputs for accountability and troubleshooting; tracking model versions and timestamps; validating outputs with human-in-the-loop reviews; and performing regular checks for errors or bias).[2]
- *Emerging Trends – AI Agents*. AI agents are autonomous systems or programs that plan, decide, and act within an environment to achieve user-defined goals without predefined rules or logic. While AI agents extend GenAI capabilities by enabling broader task automation and faster interaction with wide-ranging data sources and systems, FINRA points out that they introduce risks and challenges that could negatively impact customers, firms, and markets, including:
    - Autonomy, where AI agents may act without human validation or approval;
    - Scope and authority, as AI agents may exceed the user's intended mandate or permissions;
    - Auditability and transparency, in that multi-step reasoning can be hard to trace, hampering explainability and complicating auditability;
    - Data sensitivity, where AI agents might inadvertently store, expose, or misuse sensitive or proprietary data;
    - Domain knowledge, where general-purpose AI agents may lack the expertise needed for complex, industry-specific tasks;

- Rewards and reinforcement, where misaligned or poorly conceived reward functions can drive harmful agent decision making to the detriment of investors, firms, or markets; and
- Unique GenAI risks, including bias, hallucinations, and privacy concerns.

Firms contemplating AI agent use should evaluate whether their autonomy creates novel regulatory, supervisory, or operational obligations and adopt AI agent-specific controls accordingly. Key considerations include monitoring AI agent system access and data handling; defining human-in-the-loop oversight procedures; tracking and logging AI agent actions and decisions; and implementing guardrails to constrain or restrict AI agent behaviors, actions or decisions.

- **Cybersecurity**. FINRA continues to observe a range of sophisticated cybersecurity threats targeting member firms and their customers, such as ransomware and extortion events, system breaches involving unauthorized access to confidential firm and customer information; social engineering schemes (*e.g.*, phishing, smishing, and quishing) that redirect users to malicious sites to steal their credentials; new account fraud; account takeovers; and insider threats, where firm employees purposefully or inadvertently use their access to firms' systems to cause harm to firms and their customers. FINRA is monitoring new cyber threats to firms, notably GenAI-enabled fraud and cybercrime-as-a-service, in which criminals with technical expertise sell tools and services to others to commit sophisticated cybercrimes. FINRA identifies new effective practices to consider when assessing and managing cybersecurity threats, including:
  - *Monitor for Customer Account Takeovers*. Review and evaluate unusual activity, including wire requests to new or previously unused third parties and suspicious logins from unknown web browsers or locations, and decide whether to impose trading or funding restrictions on identified accounts;
  - *Bring Your Own Device ("BYOD")*. Implement reasonable supervisory protocols for all firm personnel with clear policies and procedures governing secure BYOD usage;
  - *Training and Security Awareness*. Conduct regular staff training on cybersecurity best practices, including how to recognize and report phishing and other social engineering attacks;
  - *Cross-Team Communication*. Encourage coordination between cyber and information technology personnel and anti-money laundering ("AML") personnel to address cybersecurity concerns and report suspicious activity; and
  - *Monitor Third-Party Vendor Risk*. Conduct ongoing oversight for risks arising from vendor relationships.
- **Amendments to Regulation S-P**. FINRA reminds firms that the SEC adopted Regulation S-P amendments that require firms' policies and procedures to include, among other things, a

program reasonably designed to spot, respond to, and recover from unauthorized access to, or use of, customer information, including steps to notify impacted individuals when their sensitive information was, or is reasonably likely to have been, accessed or used without authorization. Larger entities had until December 3, 2025, to comply with the Regulation S-P amendments, while smaller entities must comply by June 3, 2026.[3]

- **Manipulative Trading in Small-Cap, Exchange-Listed Equities**. FINRA warned in last year's report as well as in FINRA Regulatory Notice 22-25 (FINRA Alerts Firms to Recent Trend in Small-Capitalization IPOs) that certain small-cap, exchange-listed issuers have been targeted by manipulative pump-and-dump schemes in connection with initial public offerings ("IPOs"). These schemes persist and have evolved as follows:
    - The pump-and-dump occurring less often at the time of the small-cap issuer's IPO and more often months afterward, with some issuers targeted multiple times;
    - Ahead of any manipulation, nominee accounts coordinating to "funnel" shares to foreign omnibus accounts, moving a significant portion of the public float to such accounts; and
    - Well after an IPO, issuers selling large blocks of shares in privately placed secondary offerings to select foreign investors without adequate public disclosure, who then hold a large portion of the public float and may deposit the securities at U.S. brokerages or foreign institutions with accounts at U.S. brokerages.

  In October, FINRA initiated a targeted examination of practices concerning private and public offerings by small-cap, exchange-listed issuers with operations in foreign jurisdictions.[4]

- **Third-Party Risk Landscape**. Given member firms' growing dependence on third-party vendors and the rise in cyberattacks and outages involving vendors, FINRA continues to monitor associated risks through firm outreach as part of FINRA's Risk Monitoring program. FINRA also launched the Cyber & Operational Resilience ("CORE") program to identify, assess, and share cyber and technology risk intelligence directly with potentially impacted firms, including with respect to early detection of vendor-related threats, systemic technology failures, and emerging cyberattack patterns.[5]

- **Technology Management**. The Report points to effective technology management as a key factor contributing to regulatory compliance. System outages, suboptimal performance, or insufficient controls impair a firm's ability to meet its regulatory obligations. FINRA outlines effective practices related to technology management, including:
    - *Governance*. Establish a comprehensive technology governance framework with clear accountability, oversight, and documented processes to identify, assess, mitigate, and monitor technology risks across the firm.
    - *AI/Large Language Models ("LLMs")*. Implement supervision, governance, or model risk management frameworks with clear policies for AI/LLM development, deployment, use,

and monitoring, supported by comprehensive documentation as well as data quality, integrity, retention, and security.

- *IT Resiliency*. Implement and test firm and, where applicable, vendor controls to maintain acceptable service levels during disruptions of critical information technology systems or services.

FINRA also highlights new areas for effective practices relating to third-party vendors generally, such as:

- *Vendor Due Diligence*. Perform ongoing due diligence of third-party vendors supporting mission-critical systems (*e.g.*, cybersecurity, AML monitoring), including reviewing any use of GenAI in products or services.
- *Data Inventory*. Maintain an up-to-date inventory of the types of firm data third-party vendors access or store.
- *Security Monitoring*. Monitor third-party services for security vulnerabilities and potential or confirmed data breaches.
- *Data Disposition*. Incorporate procedures to return or securely destroy firm data upon the end of a third-party vendor contract.

SELECTED TOPICS

The Report addresses 21 regulatory topics organized into seven sections: Financial Crimes Prevention; GenAI: Continuing and Emerging Trends; Firm Operations; Member Firms' Nexus to Crypto; Communications and Sales; Market Integrity; and Financial Management. We highlight below certain new topics for 2026 and new content that FINRA added to previously covered topics.

FINANCIAL CRIMES PREVENTION

AML, FRAUD, AND SANCTIONS

The Financial Crimes Prevention section contains significant new content relating to AML and external fraud threats. FINRA identifies findings relating to AML deficiencies in surveillance and investigations, including:

- *Under Resourced AML Programs*. Insufficient staffing and resources, particularly after material business expansions or changes, or when presented with the emergence of new threats.
- *Escalation Failures Across Functions*. Failures to establish effective mechanisms to escalate red flags detected outside an AML program (*e.g.*, cybersecurity incidents, account compromises, account takeovers) that may need a suspicious activity report ("SAR") filing.

- *Customer Due Diligence Red Flags Ignored*. Not investigating mismatches between a customer's stated business, occupation, and financial resources and the nature or level of account activity, and not updating risk profiles or filing SARs as necessary.
- *Inadequate Training*. No ongoing, business-tailored AML training for personnel.

FINRA also highlights certain new effective practices for compliance with AML programs, including:

- *Clear AML Ownership and Communication*. Define and document AML responsibilities across individuals and business units and maintain recurring cross department communications to identify red flags. For example, this may include indicating responsibility for identifying account breaches, account takeovers, and other cyber events.
- *Targeted Training*. Provide ongoing AML training tailored to roles and responsibilities, aligned to the firm's specific risks and recent regulatory developments, and informed by Q&A results and independent testing findings.
- *Alert and Exception Report Testing*. Periodically review alerts and exception reports to ensure they function as intended, reasonably detect the suspicious activity they are designed to identify, and properly ingest required data.

The Report updates ***external fraud threat*** trends, which include disaster-related scams that exploit charitable giving intended to support victims of tragic events; investment club scams that use social media influencers to funnel victims to "clubs" for pump-and-dump schemes; and crypto confidence frauds in which bad actors build personal rapport to guide victims into phony crypto apps and websites. FINRA recommends several risk-based practices that firms should incorporate into their compliance programs to identify and mitigate such external fraud threats, such as:

- *Education*. Distribute materials to firm personnel and customers explaining common scams and available resources for assistance.
- *Integrate AML and Anti-Fraud Functions*. Foster communication and information sharing channels to identify and respond to external fraud red flags.
- *Vulnerable Customers*. Use protective holds pursuant to FINRA Rule 2165 (Financial Exploitation of Specified Adults) when financial exploitation is reasonably expected, obtain and use trusted contact information consistent with FINRA Rule 4512 (Customer Account Information), and utilize FINRA's Securities Helpline for Seniors for guidance.

FINRA highlights a continued rise in ***new account fraud*** ("NAF"), in which bad actors open accounts using stolen identities, and ***account takeovers*** ("ATOs"), in which bad actors use stolen customer login information to gain access to existing accounts. Fraudsters are using GenAI to defeat customer identification ("ID") verification processes to commit NAF and ATOs in a number of ways, including through social engineering, AI-generated voices, AI-augmented IDs, and GenAI-generated "deepfake" images and videos impersonating a victim.

FINRA provides effective practices firms may consider incorporating into their risk-based compliance programs to mitigate the threat of such frauds, especially where fully online onboarding processes that rely on automated account opening or customer verification services are used. These include:

- Provide customer education regarding identity-theft protections and periodically remind them to update login information, especially after known breaches;
- Use additional authentication when anomalies (*e.g.*, unusual locations or Internet Protocol or behavior) are detected, including callbacks, likeness checks, and multi-factor authentication;
- Temporarily block or limit outgoing transfers from potentially compromised accounts, particularly after password or contact changes or out-of-pattern, high-risk activity is detected;
- When one fraudulent attempt is detected, review contemporaneous applications or accounts with similar attributes; and
- Participate in industry, regulatory, and law-enforcement anti-fraud networks and mailing lists to stay current on emerging threats and mitigation techniques.

FIRM OPERATIONS

OUTSIDE BUSINESS ACTIVITIES AND PRIVATE SECURITIES TRANSACTIONS

The Report provides an update on proposed FINRA Rule 3290 (Outside Business Requirements), which aims to streamline the obligations in FINRA Rules 3270 (Outside Business Activities of Registered Persons) and 3280 (Private Securities Transactions of an Associated Person). In July 2025, FINRA's Board of Governors approved a revised version of the rule for filing with the SEC, and as of December 2025, FINRA staff are preparing the resubmission.

BOOKS AND RECORDS

FINRA observed new trends in books and records violations, including:

- *FOCUS Reports, Net Capital, and Reserve Calculations*. Inaccurate books and records (*e.g.*, general ledger, trial balance) leading to discrepancies in net capital and reserves formula calculations. Firms have reported incorrect net capital, aggregate indebtedness, revenue, liabilities, and reserve computations, resulting in inaccurate FOCUS filings and violations of SEC Rules 17a-3, 17a-4, and 17a-5, as well as FINRA Rule 4511.
- *Electronic Communication Retention Failures*. Not capturing, reviewing, and archiving firm business electronic communications of associated persons—especially part-time Chief Compliance Officers and Financial and Operations Principals ("FINOPs")—who use third-party vendor email addresses.

MEMBER FIRMS' NEXUS TO CRYPTO

FINRA urges firms to closely track and respond to rapid market, legislative, and policy developments in crypto assets. (Notably, the SEC dropped crypto assets from its 2026 examination priorities; see our Legal Update here). Recent developments include multiple SEC staff statements and guidance from the Divisions of Corporation Finance and Trading and Markets.

FINRA emphasizes recurring crypto-related compliance issues across several rules, particularly under FINRA Rule 2210 (Communications with the Public), where influencer and social media promotions were unfair, unbalanced, or misleading, and firms failed to disclose when crypto assets were offered by a non-member firm. FINRA identifies certain effective practices that firms should consider before recommending unregistered offerings of crypto assets that are securities, such as understanding the issuer's business and planned use of proceeds, and review disclosed risk factors and conflicts of interest. Finally, FINRA encourages firms to notify it of new or planned digital asset activities and to contact their Risk Monitoring Analyst with questions.

COMMUNICATIONS AND SALES

The Communications and Sales section of the Report adds guidance relating to communications with the public, Regulation Best Interest ("Reg BI"), private placements, and annuities securities products.

The Report contains new material relating to the use of ***social media influencers and mobile apps***. FINRA observed that firms have inadequate supervision of social media influencers by failing to review and approve influencers' firm-related static content before posting, and by not supervising influencer communications in interactive forums to the same standard as firm communications. Firms also failed to retain retail communications posted by influencers on the firm's behalf. Finally, some firms provided false, misleading, inaccurate, or unbalanced information in their mobile apps, including failing to disclose or inaccurately disclosing the risks of loss associated with certain options transactions.

With respect to ***Reg BI***, the Report identifies several findings related to firms failing to maintain or enforce written policies and procedures for account recommendations by omitting clear guidance on the factors to evaluate—such as account costs, services provided, and whether services would be duplicative—when recommending specific account types, and by not specifying the supervisory steps needed to determine whether an account-type recommendation was in the customer's best interest. FINRA continues to see issues in ***private placement offerings*** of pre-IPO funds, including potentially fraudulent conduct such as material misrepresentations and omissions about sales compensation tied to recommendations. Firms have also failed to conduct reasonable due diligence, for example by failing to verify that a fund actually possessed or could access the pre-IPO shares it claimed to hold, and by not adequately understanding the costs associated with acquiring those shares.

Finally, concerning **annuities securities products**, FINRA identified violations of Reg BI's Care Obligation relating to recommended surrenders and withdrawals, including failures to consider the costs of terminating variable annuity living benefits and riders when recommending replacements or exchanges, and recommending partial withdrawals or full surrenders from registered index-linked annuities "mid-segment" without considering interim value risk.

MARKET INTEGRITY

The Market Integrity section of the Report discusses: the Consolidated Audit Trail ("CAT"); fair pricing obligations for fixed income transactions; and extended hours trading.

The Report includes new content on supervisory deficiencies relating to ***CAT reporting***, including selecting review samples that lacked diversity in order and event types when reviewing CAT reports, and failing to use proportionate samples across all desks, aggregation units, business lines, and order flows when checking for reporting accuracy.

With respect to ***fixed income–fair pricing***, FINRA identified that firms incorrectly determined the prevailing market price ("PMP") by failing to follow the contemporaneous cost presumption and the required waterfall under FINRA Rule 2121 (Fair Prices and Commissions) and Municipal Securities Rulemaking Board Rule G-30 (Prices and Commissions), instead relying on third-party software to set PMP and then not conducting compliance or supervisory reviews of trades the software flagged for excessive mark-ups or mark-downs relative to that PMP.

Finally, with respect to ***extended hours trading***, FINRA highlights as an effective practice implementing supervisory processes tailored to overnight trading that reflect venue-specific price bands and include reviews for trades executed outside those bands or activity that appears intended to set the bands in a potentially manipulative manner.

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 deficiencies in financial controls, such as inaccurate books and records (*e.g.*, FOCUS filings and general ledgers) and improper classification or accrual of expenses and liabilities, as well as inadequate processes or supervision for underwriting commitments, such as failing to document that the commitment was fully sold before discontinuing open contractual commitments ("OCC") charges. FINRA also reminds member firms about annual financial reporting and submission requirements for SEC Rule 17a-5(d) annual reports, including that oaths or affirmations must be administered by authorized persons and that compliance reports or exemption reports must be executed by the person making the oath or affirmation.

With respect to ***liquidity risk management***, FINRA continues to prioritize strong liquidity and funding risk management and uses the Supplemental Liquidity Schedule ("SLS") to monitor adverse liquidity signals at firms with significant customer and counterparty exposures. FINRA has observed recurring SLS reporting errors, including:

- Misidentifying counterparties (*e.g.*, listing agent lenders rather than underlying principals), or omitting clearing organizations on novated repurchase and reverse repurchase agreements;
- Providing incomplete details on noncash securities lending and clearing deposits (*e.g.*, missing dates, using month-end amounts, including weekends); and

- Failing to complete or accurately report "Total Available Collateral in Broker-Dealer's Custody."

The Report reminds firms that the SEC extended to June 30, 2026, the compliance date for amendments requiring certain firms to perform daily (rather than weekly) reserve formula computations, a change that can materially affect funding and liquidity. Firms should evaluate impacts on funding needs, update stress testing and contingency funding plans accordingly.

With respect to ***customer protection***, FINRA identified as a finding improper treatment of free credit balances by transferring customer funds to third parties without appropriate specific authorization or not following the terms of the authorization. Firms also failed to provide FINOPs—especially part-time or contracted personnel—adequate access to books and records needed to perform required duties, and did not sufficiently complete reconciliations with external parties to verify that books and records accurately reflected the proper ownership and location of customer assets. Finally, FINRA reminds firms that the SEC extended to June 30, 2026, the compliance date for amendments requiring certain firms to move from weekly to daily customer reserve computations under SEC Rule 15c3-3, but the separate amendment allowing firms that perform daily computations to apply a 2% (instead of 3%) reduction to aggregate debit items remains in effect.

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

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

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

JOSHEA MARK
+1 212 506 2661
JMARK@MAYERBROWN.COM

---

[1] See our Legal Update for a discussion of the SEC's 2026 examination priorities.
[2] See our Legal Update for additional details regarding regulatory obligations when using AI.
[3] See our Legal Update for additional details regarding these amendments.
[4] See our blog post regarding FINRA's targeted examination of small-cap, exchange-listed issuers.
[5] See our Legal Update regarding FINRA's focus on third-party providers.