Articles + Publications | December 17, 2025

Key Takeaways from FINRA's 2026 Annual Regulatory Oversight Report

WRITTEN BY

Jay A. Dubow | Ghillaine A. Reid

The Financial Industry Regulatory Authority's (FINRA) 2026 Annual Regulatory Oversight Report is the most current and comprehensive statement of FINRA's priorities and expectations for member firms. It does not create new legal obligations, but it is clearly designed as an exam and enforcement roadmap. The 2026 Report weaves together FINRA's FINRA Forward modernization program, new and evolving risks (especially cyber?enabled fraud and generative AI (GenAI)), and detailed observations on firms' supervisory, operational, and financial controls. Firms should use it as a structured checklist for 2026 risk assessments, revisions to written supervisory procedures (WSPs), and enhancements to testing, surveillance, and training.

FINRA Forward and the Role of the Report

FINRA Forward, launched in 2025, underpins much of this year's Report. It has three pillars: modernizing FINRA's rules to better reflect current markets, "empowering member firm compliance" with more tools and feedback, and intensifying focus on cybersecurity and fraud. Organizationally, FINRA has unified Member Supervision, Market Oversight, and Enforcement into a single Regulatory Operations function, which means firms should expect more integrated, cross?silo supervision and enforcement.

The Report is explicitly positioned as an evolving reference library. It updates prior topics, adds new ones (notably a dedicated GenAI section), and highlights "effective practices" and resources. Firms are encouraged to read it selectively, focusing on areas relevant to their business lines and risk profile, but examiners will reasonably expect that the Report has informed the firm's compliance planning.

Cybersecurity and Cyber?Enabled Fraud

Cyber remains at the top of FINRA's agenda. The Report ties cyber risk directly to Regulation S?P (privacy and safeguarding), Regulation S?ID (identity theft red flags), FINRA Rule 3110 (supervision), Rule 4370 (BCP), and Exchange Act books?and?records rules. It emphasizes the 2024 amendments to Regulation S?P, which require a written program to detect, respond to, and recover from unauthorized access to "sensitive customer information," including customer notification. Larger firms were to have complied by December 3, 2025, while smaller firms have until June 3, 2026.

Substantively, FINRA continues to see ransomware and extortion events, data breaches, phishing/smishing/quishing, new account fraud, account takeovers, account impersonation and imposter sites. Relationship investment scams, often initiated via text or social media, are a particular concern. The Report also

flags GenAI?enabled threats such as deepfake audio/video and AI?generated documents/polymorphic malware, as well as “cybercrime?as?a?service” tools that allow less technical actors to launch sophisticated attacks.

FINRA’s “effective practices” now look more like baseline expectations: multifactor authentication for staff and customers; monitoring for unusual logins and payment requests; domain and social media impersonation surveillance; outbound data?loss controls; network segmentation; BYOD governance; routine training; cross?team coordination between cyber and anti-money laundering (AML); and structured vendor risk management. The practical question is no longer whether these controls exist but whether they are formally documented, consistently implemented and demonstrably tested.

AML, External Fraud, and Identity?Based Threats

The Report devotes extensive attention to AML (FINRA Rule 3310) and “external fraud” threats. FINRA continues to find AML programs that are not properly tailored to firms’ businesses, that under?resource monitoring and investigations (especially after business growth), and that fail to escalate red flags from outside the AML function (*e.g.*, cyber alerts, clearing firm inquiries).

FINRA highlights evolving fraud patterns: disaster?related donation scams; social media “investment clubs” used to drive pump?and?dump activity; gold bar courier scams in which customers are convinced to liquidate portfolios and hand physical metals to “couriers” crypto confidence schemes relying on phony apps; and mail?theft?related check fraud. In parallel, FINRA sees persistent new account fraud and account takeovers, increasingly enabled by GenAI through highly targeted phishing, voice clones used in call?center interactions, AI?generated identity documents, and deepfake “selfies” that defeat automated KYC.

The Report expects firms to incorporate these typologies into their risk?based AML and fraud programs, CIP/CDD controls, independent testing, and training. It emphasizes the importance of robust identity verification at onboarding and during investigations, careful scrutiny of omnibus accounts and small?cap offerings, clear escalation paths for suspicious activity, and use of available tools such as FINRA Rule 2165 (temporary holds) and trusted contact information when exploitation is suspected.

GenAI: Governance, Risk, and AI Agents

For the first time, FINRA devotes a standalone section to GenAI. The central message is that FINRA’s rules are technology?neutral, meaning using GenAI does not change a firm’s obligations under supervision, communications, recordkeeping, outsourcing, or fair?dealing standards. However, GenAI amplifies many existing risks and introduces new governance challenges.

FINRA notes that most current use cases are internal and efficiency?oriented such as summarization and information extraction, conversational assistants, coding support, synthetic data generation, and workflow automation. But even internal deployments can impact supervisory systems and decision?making. The Report warns about “hallucinations” (confident but incorrect outputs) and bias (skewed outputs due to limited or outdated training data) and expects firms to test for and manage these risks, especially where GenAI touches regulatory analysis, surveillance, customer communications or product design.

Firms are urged to implement enterprise?level GenAI oversight, with formal review and approval processes for new use cases; model risk management adapted to GenAI; testing for accuracy, reliability, privacy, and bias; logging of prompts and outputs; and appropriate human?in?the?loop review. FINRA also flags AI "agents," autonomous systems that plan and execute tasks, as an emerging concern.

Third?Party and Technology Risk

The Report also reinforces FINRA's longstanding view that outsourcing does not outsource responsibility. Firms must maintain a supervisory system reasonably designed to oversee activities performed by vendors, including technology, AML monitoring, cybersecurity, and key back?office functions. FINRA notes more frequent cyber incidents and outages at vendors and stresses the importance of understanding concentrations of systemic risk where many firms rely on the same providers.

In 2025, FINRA enhanced its own capabilities by launching Cyber & Operational REsilience (CORE), which collects and shares cyber and technology risk intelligence with potentially affected firms. The Report encourages firms to keep FINRA apprised of changes in critical vendors and to integrate vendor?related scenarios into incident response planning and testing.

Effective practices include maintaining detailed vendor inventories; structured initial and ongoing due diligence that covers security, resilience and any use of GenAI; contractual limits on how vendor tools may consume and use firm and customer data; continuous monitoring for vulnerabilities and breaches; coordinated incident response with vendors; and disciplined off?boarding to ensure data is returned or destroyed and access is revoked.

Crypto Assets

The Report reiterates that FINRA's focus is on member firms' crypto activities, especially where crypto assets are securities or are offered and sold as investment contracts. FINRA highlights enforcement issues around communications (Rule 2210) that misstate or omit risks, overstate protections (*e.g.*, SIPC coverage), or make unsound comparisons to traditional investments, including content disseminated through influencers.

FINRA also continues to see deficiencies in firms' due diligence on crypto?related private placements and products, AML programs that do not adequately address crypto?related risks, and operational issues such as improper ACATS rejections when customers maintain associated crypto accounts with affiliates. The Report expects firms to understand the legal basis for unregistered offerings, the mechanics and risk profile of crypto securities, and to use on?chain analytics where appropriate in AML and fraud monitoring.

Retail Communications, Social Media, and AI?Generated Content

FINRA's communications findings have a strong digital flavor. Many firms lack robust supervision and recordkeeping around social media influencers acting on the firm's behalf, including failure to pre?approve static content, supervise interactive content, or archive posts as required. Mobile app interfaces and push notifications are another area of concern, particularly where they do not adequately explain products (options, margin, complex or crypto?linked strategies), understate risk, or use gamified "nudges" that are promissory or misleading.

When GenAI is used to draft or deliver communications, FINRA expects full compliance with existing standards: communications must be fair and balanced, consistent with products actually offered, and properly supervised and retained. Chatbots interacting with customers are treated as firm communications and must be supervised and archived accordingly. References to AI?enabled products or services must accurately reflect how AI is used and balance potential benefits with clear discussion of risks.

Regulation Best Interest and Complex Products

Regulation Best Interest (Reg BI) continues to be a central focus. The Report details failures under the Care Obligation (inadequate product due diligence, recommendations inconsistent with customer profiles, insufficient consideration of costs and reasonably available alternatives, weak documentation of account?type and rollover recommendations), as well as under the Conflict of Interest, Disclosure, and Compliance Obligations. Many of these issues are most acute around complex or higher?risk products, including variable annuities, RILAs, options, and certain private placements.

In private placements, FINRA emphasizes that firms must conduct reasonable investigations of issuers, offerings and management; respond to red flags; maintain evidence of due diligence; and comply with private placement filing requirements. FINRA notes continuing concerns with pre?IPO fund offerings, including misstatements about holdings and access to pre?IPO shares.

In the annuities space, FINRA highlights problematic exchange patterns, including transactions that increase fees, restart surrender periods or forfeit valuable riders without sufficient benefit, and notes that many firms lack robust WSPs, data and surveillance for RILA recommendations. As an effective practice, FINRA suggests applying Rule 2330?style heightened controls to RILAs, with documented rationales, principal review, and exchange trend monitoring.

Market Integrity: CAT, Best Execution, Manipulation, Market Access, and Extended Hours

The market integrity section touches several pillars. For the Consolidated Audit Trail (CAT), FINRA continues to find incomplete, inaccurate and untimely reporting, weak error correction and insufficient oversight of third?party reporting agents. Firms should be able to map internal records to CAT fields, systematically review CAT feedback, and sample reported data against trade blotters.

Best execution under FINRA Rule 5310 remains a core obligation. FINRA expects “regular and rigorous” reviews of execution quality that genuinely compare venues and order types, consider the impact of payment for order flow and venue incentives, and result in modifications or documented justifications where appropriate. The Report also highlights continuing inaccuracies and omissions in Rule 606 order routing disclosures and expects firms to have WSPs that ensure accuracy, completeness, and timely publication.

Manipulative trading, particularly in small?cap exchange?listed issuers, remains a high?priority surveillance area. FINRA describes evolving pump?and?dump schemes that exploit nominee accounts, foreign omnibus accounts, undisclosed secondary offerings and, increasingly, account takeover?driven purchases. Firms are expected to tailor surveillance to their business and customer base and to integrate these patterns into AML and market abuse monitoring.

Under the Market Access Rule (SEA Rule 15c3?5), FINRA expects pre?trade financial and regulatory risk controls that are calibrated to firms' business models and demonstrably reasonable, with clear documentation and controls over intra?day adjustments. Overreliance on venue?provided controls, without firm?level oversight, is viewed as inadequate. Firms are also expected to conduct holistic post?trade reviews for manipulative activity and document annual effectiveness reviews.

Extended?hours trading triggers familiar obligations: clear and prominent risk disclosures under Rule 2265, incorporation of extended?hours orders into best execution, CAT and TRF reporting, and supervisory processes that address lower liquidity, wider spreads and venue?specific price bands overnight. FINRA also expects firms to think about operational readiness and customer support during overnight trading sessions.

Financial Responsibility, Liquidity, and Customer Protection

The Report underscores ongoing issues and new requirements under the net capital rule, customer protection rule, and liquidity management expectations. FINRA continues to identify improper revenue and expense recognition, misclassified assets and liabilities, and incorrect haircuts or OCC charges, particularly in underwriting arrangements. It points to recent SEC actions requiring EDGAR submission of annual reports, forthcoming XBRL tagging requirements for FOCUS reports, and amendments to customer and PAB reserve computations. Most notably, the requirement for certain firms to move to daily reserve computations by June 30, 2026, with corresponding funding and liquidity implications.

FINRA's Supplemental Liquidity Schedule (SLS) has become an important supervisory tool, and the Report notes recurring SLS errors, such as misidentified counterparties, incomplete reporting of securities borrowing and lending, and inaccurate collateral data. Firms are expected to maintain liquidity governance frameworks, run stress tests that reflect both firm?specific and market?wide shocks, and maintain contingency funding plans that realistically account for contractual covenants and the potential unavailability of certain funding sources under stress.

Under the Customer Protection Rule (Rule 15c3?3), FINRA continues to observe weaknesses in reserve formula computations, customer vs. noncustomer classifications, management of suspense items, possession or control of customer securities, and reconciliations with external custodians. FINRA stresses the importance of experienced FINOPs with appropriate access to books and records and of ongoing variance analyses and control testing.

Senior Investors and Trusted Contacts

The Report reaffirms FINRA's focus on senior and vulnerable investors. It notes that many firms still fail to make reasonable efforts to obtain trusted contact information (Rule 4512), do not provide customers with clear disclosures about how trusted contacts may be used, and rely on Rule 2165 (temporary holds) without documented training or internal review procedures. FINRA encourages firms to integrate senior investor protection into their broader fraud and AML frameworks, including escalation protocols that involve trusted contacts, Adult Protective Services and law enforcement where appropriate, and to provide staff with practical "playbooks" and training on recognizing exploitation and diminished capacity.

Practical Implications

In practice, the Report functions as a detailed “to?do list” for 2026. Firms should map its topics to their own business activities, update risk assessments, and then prioritize enhancements to WSPs, surveillance, testing, and training. This is particularly important in the areas of cyber and fraud (including GenAI?enabled threats), GenAI governance, Reg BI and complex products, digital communications, market integrity controls, liquidity management, and senior investor protection. While the Report does not introduce new binding rules, it sets out the standards against which FINRA will evaluate whether a firm’s compliance program is reasonable, risk?based and responsive to today’s investor and market risks.

RELATED INDUSTRIES + PRACTICES

- Securities Investigations + Enforcement
- Securities Litigation
- White Collar Litigation + Investigations