Debevoise & Plimpton

Debevoise In Depth

FINRA’s 2026 Regulatory Oversight Report: Continued Focus on Generative AI and Emerging Agent-Based Risks

December 12, 2025

On December 9, 2025, FINRA released its 2026 FINRA Annual Regulatory Oversight Report (the “2026 Report”). The 2026 Report contains a standalone section on Generative AI (“GenAI”) that substantially expands upon the topic from last year’s publication. In particular, the 2026 Report builds on FINRA’s prior AI guidance by reminding firms of their continuing regulatory obligations with respect to GenAI, describing how firms are using GenAI, articulating expectations for GenAI governance, testing, and monitoring, and, for the first time, discussing the risks of AI agents.

In this Debevoise Client Update, we summarize the 2026 Report’s latest GenAI guidance and offer practical considerations for firms evaluating or expanding GenAI and agentic AI use cases.

Regulatory Obligations for GenAI

The 2026 Report reiterates that FINRA’s regulatory framework is technology-neutral and that firms remain responsible for compliance when using GenAI tools within their businesses.

The 2026 Report highlights that GenAI may implicate rules relating to supervision, communications, recordkeeping, and fair dealing. For example, the 2026 Report notes that when firms integrate GenAI into supervisory systems, they should ensure that their policies and procedures address the reliability, integrity, and accuracy of the models on which they rely.

GenAI Use Cases Observed Across Member Firms

The 2026 Report reflects the substantial expansion of GenAI use among member firms in just 12 months. FINRA’s 2025 report referenced only three GenAI use cases that firms had implemented:

- *Summarization*: Summarizing information from multiple information sources into one document.

- *Analysis*: Conducting analyses across disparate data sets. For example, a firm may use GenAI to assess and validate the accuracy of reported transactions using various source documents.

- *Policy Retrieval*: Enabling employees to retrieve relevant portions of policies and procedures via GenAI.

The 2026 Report observes that summarization remains the top GenAI use case but also adds a dozen use cases to the list:

- *Conversational AI & Question Answering*: Systems that provide interactive, natural-language responses through chatbots, virtual assistants, or voice interfaces.

- *Sentiment Analysis*: Capabilities that assess the tone or sentiment of text as positive, neutral, or negative.

- *Translation*: Tools that translate text between languages or convert audio to text and vice versa.

- *Content Generation & Drafting*: Technologies that create written materials such as documents, reports, or marketing content.

- *Classification & Categorization*: Systems that organize data, documents, or transactions into predefined groups.

- *Workflow Automation & Process Intelligence*: GenAI solutions that optimize business processes through intelligent routing, automation, and dynamic agents.

- *Coding*: Tools that generate software code based on specified inputs or objectives.

- *Query*: Applications that allow users to retrieve information from structured databases using natural-language inputs.

- *Synthetic Data Generation*: Techniques that create artificial datasets that resemble real-world data for use in modeling or testing.

- *Personalization & Recommendation*: Systems that tailor content, products, or services to individual customer preferences.

- *Data Transformation*: Capabilities that convert unstructured data into standardized formats.

- *Modeling & Simulation*: Applications that automate modeling, forecasting, scenario analysis, and related simulations.

Considerations for Firms Contemplating GenAI Use

The 2026 Report emphasizes that the increased use of GenAI introduces risks that require effective governance, supervision, testing, and additional expectations for ongoing monitoring. The 2026 Report encourages firms contemplating the use of GenAI to consider the following:

- *Enterprise-Level Governance and Risk Assessment*: Developing supervisory processes for the development and use of GenAI at the enterprise level. This process includes identifying and mitigating risks such as hallucinations, which the 2026 Report defines as "instances where the model generates information that is inaccurate or misleading, yet is presented as factual information." For example, a model that misinterprets a regulatory requirement or misstates client information could lead to flawed downstream decisions. The 2026 Report also notes that bias may arise from limited, outdated, or skewed training data, potentially influencing GenAI outputs in ways that reflect historical data patterns rather than current conditions. FINRA further encourages firms to assess whether their cybersecurity programs adequately address risks associated with both internal and third-party use of GenAI, including how the firm's technology stack detects or responds to attempts by threat actors to exploit AI or GenAI as part of an attack vector.

- *Supervision and Governance Frameworks*: Implementing formal review and approval processes that incorporate both business and technology expertise, and establishing clear policies and procedures for developing, implementing, using, and monitoring GenAI. Comprehensive documentation throughout the lifecycle of a GenAI tool also remains an important component of effective governance.

- *Testing*: Understanding the capabilities, limitations, and performance of GenAI models through robust testing. Testing should address considerations such as privacy, data integrity, reliability, and accuracy. As a practical matter, firms may consider testing both before deployment and as models or use cases evolve, to understand how a GenAI model performs under typical conditions and to identify situations in which the model may produce inconsistent or unreliable results.

- *Ongoing Monitoring and Human-in-the-Loop Review*: Monitoring GenAI outputs on an ongoing basis to confirm that deployed solutions continue to perform as expected and support compliant behavior. The 2026 Report provides significantly more specificity than FINRA's 2025 report on the parameters of such monitoring, including reviewing prompts, responses, and outputs over time, maintaining prompt and output logs for accountability and troubleshooting, tracking which model version was used and when, and conducting validation and human-in-the-loop review with regular checks for errors or bias.

Emerging Trend: AI Agents

AI agents are a new focus in the 2026 Report, which defines AI agents as "systems or programs that are capable of autonomously performing and completing tasks on behalf of a user." The 2026 Report highlights several risks to investors, firms, and markets from AI agents:

- *Autonomy and Scope Creep*: Agents may act without human validation and may take actions that exceed the user's actual or intended scope or authority.

- *Auditability and Transparency*: Multi-step reasoning or complex chains of agent actions may be difficult to reconstruct, complicating auditability.

- *Sensitive Data Handling*: Agents working with sensitive or proprietary data may unintentionally retain or reveal that information.

- *Insufficient Domain Expertise*: General-purpose agents may lack the domain knowledge required to perform complex or industry-specific tasks reliably.

- *Misaligned Incentives*: Misaligned or poorly designed reward functions may cause the agent to optimize behavior in ways that could negatively affect investors, firms, or markets.

- *Unique GenAI Risks*: Existing risks, such as bias, hallucinations, and privacy challenges, remain applicable to agent outputs.

To address these risks, FINRA encourages firms exploring AI agents to evaluate whether their autonomy creates novel regulatory, supervisory, or operational considerations and to develop agent-specific supervisory processes, including:

- monitoring agent system access and data handling;

- determining where human-in-the-loop oversight is required;
- tracking agent actions and decisions; and
- establishing guardrails or control mechanisms to constrain agent behavior.

These themes reflect FINRA's broader message that emerging GenAI tools, including AI agents, are subject to existing regulatory expectations and therefore require supervisory processes tailored to their design and use, and, as we have discussed here, firms remain responsible for recommendations and decisions influenced by GenAI.

Key Takeaways

Given FINRA's expansive guidance on GenAI and increasing scrutiny of agentic AI, firms may consider adopting the following GenAI governance and oversight measures:

- **Strengthen Testing and Monitoring**. Firms may want to revisit their GenAI testing and monitoring programs in response to FINRA's expanded expectations. This process may include undertaking structured pre-deployment testing tailored to evaluate reliability, accuracy, and other performance characteristics, as well as establishing ongoing monitoring of prompts, outputs, and model behavior to confirm that GenAI tools continue to operate as intended.
- **Maintain Accurate and Balanced AI-Related Disclosures**. As firms expand their use of GenAI and agentic AI, they may want to build additional processes to ensure that descriptions of these tools in customer communications and marketing materials remain accurate, comprehensive, and not overstated. As we have discussed here, the SEC and DOJ have brought AI washing charges against financial services firms for misstatements and omissions in connection with AI use, so building safeguards to test and ensure the accuracy of statements about AI's capabilities and benefits can help reduce this enforcement risk.
- **Address Cybersecurity and Data Governance**. Given FINRA's focus on the cybersecurity and data-handling risks associated with GenAI and AI agents, firms may want to incorporate these technologies into broader cybersecurity and data governance programs. Depending on the use case, this process may include reviewing access controls, data-handling expectations, and other safeguards to account for GenAI-specific risks.

- **Train Personnel and Provide Approved Enterprise GenAI Tools.** As firms operationalize GenAI programs, training supervisors, compliance personnel, and staff on GenAI's capabilities and limitations, and providing approved enterprise GenAI tools, will be important to GenAI risk management. Clear expectations and controls may help reduce the risk of inconsistent, unsupervised, and off-channel GenAI usage.

* * *

Please do not hesitate to contact us with any questions.

Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandrasekhar@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

Jeff Robins
Partner, New York
1 212 909 6526
jrobins@debevoise.com

Kristin A. Snyder
Partner, San Francisco
+1 415 738 5718
kasnyder@debevoise.com

Matt Kelly
Counsel, New York
+1 212 909 6990
makelly@debevoise.com

Jeremy I. Liss
Associate, New York
+1 212 909 6687
jiliss@debevoise.com

Ned Terrace
Associate, New York
+1 212 909 7435
jkterrace@debevoise.com

Achutha N. Raman
Law Clerk, New York
+1 212 909 6106
anraman@debevoise.com

This publication is for general information purposes only. It is not intended to provide, nor is it to be used as, a substitute for legal advice. In some jurisdictions it may be considered attorney advertising.