FINRA's 2025 Regulatory Oversight Report: Focus on Artificial Intelligence

February 5, 2025

On January 28, 2025, FINRA released its 2025 FINRA Annual Regulatory Oversight Report (the "Report"). As was the case in 2024, the Report highlights continuing and emerging trends in artificial intelligence ("AI") in the financial services sector, among other topics. In this Debevoise Client Update, we review the Report's discussion of common generative AI ("Gen AI") use cases, existing FINRA rules that are applicable to Gen AI technology, and FINRA's guidance for firms contemplating the use of Gen AI, including practices for communications derived from and about Gen AI. We also provide our key takeaways from the Report.

Common Uses of Gen AI by Firms

FINRA notes that firms are proceeding "cautiously" in employing Gen AI technology and, when doing so, are typically using third-party vendor-supported Gen AI tools, primarily to increase efficiency of internal functions. FINRA has observed the following Gen AI uses:

- **Summarization:** Summarizing information from multiple information sources into one document.
- **Analysis:** Conducting analyses across disparate data sets. For example, a firm may use Gen AI 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 Gen AI.

FINRA Rules Applicable to Gen AI Technology

The Report reiterates FINRA's intention that its rules be technologically neutral and emphasizes that FINRA's rules still apply when firms use Gen AI technology. As we have discussed, FINRA has previously explained in regulatory notice 24-09 that the application of Rule 3110 (Supervision) in the Gen AI context means that firms using Gen AI tools as part of their supervisory systems should have policies and procedures that address technology governance (including model risk management), data privacy and integrity, and reliability and accuracy of the AI model. FINRA's earlier notice underscored that its rules apply regardless of whether firms develop their own Gen AI tools or use third-party solutions.

Guidance for Firms Contemplating Using Gen AI Tools

The Report offers various considerations for firms contemplating using Gen AI tools and technologies, including:

- **Enterprise-level supervision:** Supervising Gen AI use on both the enterprise level and by individual associated persons.
- **Risk assessment and mitigation:** Identifying and mitigating risks associated with Gen AI, such as accuracy or bias.
- **Third-party risk management:** Developing ways to manage compliance risks associated with the deployment of third-party foundational models and the use of third-party software that may have Gen AI embedded therein. This process may involve asking potential third-party vendors if they incorporate Gen AI into their products or services and, if so, evaluating and, as necessary, updating contracts with these vendors to comply with any regulatory and third-party contractual obligations. For example, the Report provides that firms may consider adding language that prohibits firm or customer sensitive information from being ingested into a vendor's open-source Gen AI tool. We have previously written about these and other AI vendor risk management issues.
- **Cybersecurity risks:** Assessing whether the firm's cybersecurity program considers cybersecurity risks from the use of Gen AI. Such risks may include risks associated with the use of Gen AI by both the firm and its third-party vendors, including leakage of customer personal information and the firm's proprietary information that employees may provide via Gen AI prompts.

Communications with the Public

The Report identifies effective practices for communications both derived from and about Gen AI. Specifically, the Report identifies procedures for:

- **Gen AI-generated communications:** Firms using Gen AI to generate or otherwise assist in creating communications to customers should review these communications to ensure they comply with applicable federal securities laws and regulations, as well as FINRA rules. In separate guidance about its Advertising Regulation, FINRA has noted that firms are responsible for the content of communications created using AI, and in doing so must abide by supervision and applicable recordkeeping requirements, as well as content standards in FINRA Rules 2210 and 2200. These rules require that communications be fair and balanced and prohibit the inclusion of false, misleading, promissory, or exaggerated statements or claims.

- **Chatbot communications:** Firms using Gen AI to create or assist in creating chatbot communications that interact with investors should ensure that these communications are subject to appropriate supervision and that the chat sessions are appropriately retained in accordance with SEC and FINRA rules.

- **Retail communications about AI:** Firms should ensure that communications with retail customers that mention AI tools, AI services, or financial products that rely on AI management accurately describe how these offerings incorporate AI technology. Communications should also appropriately balance the discussion of potential benefits of AI with risks. We've previously written about SEC enforcement against AI washing here and here.

Adversarial Uses of Generative AI

For the first time this year, the Report also highlights threat actor usage of Gen AI to increase the number, credibility, or severity of attacks members now face. The Report urges firms to consider employee training about heightened fraud and cyber risks presented by adversarial use of generative AI and whether their cybersecurity programs consider using technology tools, data provenance, and processes to identify such risks. The Report observes that threat actors have used Gen AI to generate fake content such as deepfakes that may bypass authentication, create polymorphic malware that shapeshifts to evade detection, and develop malicious tools without sophisticated technical ability. It also lists ways in which threat actors have exploited Gen AI to amplify existing cybersecurity threats (such as account takeovers, BECs, ransomware

attacks, and other types of social engineering schemes). We've previously discussed how other regulators, such as NYDFS and Hong Kong's SFC, have similarly highlighted risks from threat actors' use of AI.

Key Takeaways

The Report highlights FINRA's continued focus on Gen AI and its efforts to identify and mitigate risks associated with this emerging technology. With that in mind, firms may want to consider the following measures:

- **Establishing a Gen AI risk assessment program and inventory:** While the Report focuses on two main areas of Gen AI use, communications and analysis, uses of Gen AI across different functions—not just core business and communications—can generate risk, especially cybersecurity risk. As we've previously discussed, firms should consider implementing a Gen AI governance program that (1) identifies low-risk AI uses cases that do not need a robust compliance review and do not need to be recorded in any AI inventory (*e.g.*, using Gen AI to summarize and translate public documents), (2) identifies prohibited use cases and ensures that there are no such use cases in production (*e.g.*, using a Gen AI-based chatbot that provides investment advice without human review), (3) identifies the risks associated with other Gen AI use cases, along with the appropriate mitigation measures to address those risks, and (4) keeps track of higher-risk Gen AI use cases in production to ensure that their risks, including regulatory compliance risks, remain sufficiently mitigated.

- **Defining AI consistently and truthfully:** To avoid claims of misrepresenting AI or AI usage, firms should consider creating a definition of AI that is used for both internal and external purposes and aligns to the company's actual AI capabilities and use cases. In tandem, firms should also develop policies and procedures to make sure disclosures about AI are accurate, especially with respect to marketing. Doing so will help mitigate the risk that the company will characterize something as AI externally that is not considered AI internally—a misalignment that could be interpreted as misleading.

- **Identifying vendor risks**: In tackling vendor risk, firms should be clear about what type of AI usage is implicated in the vendor's product or service. For example, is the vendor an LLM provider or an advertising firm that may use AI internally but indirectly in delivering its services? Firms should then consider creating a checklist of potential risks that the company will contemplate when engaging an AI vendor. For each risk that can be addressed through contract, consider whether it is possible to have a playbook with model diligence questions, ideal contract terms, and

acceptable fallback terms. Consider also organizing these risks into standard risks (*i.e.*, those that will be addressed for all AI vendor engagements) and nonstandard risks (*i.e.*, those that will only need to be addressed in specific contexts) and identifying which risks are covered by other diligence efforts (cyber, privacy, etc.) as opposed to those risks that are only addressed through AI-specific diligence. Finally, consider whether there are any specific regulatory risks (*e.g.*, regulatory compliance with hiring, lending, or biometric laws) that will require review and sign off from specific subject-matter experts, such as the legal team, compliance staff, or HR.

- **Assess significant AI tools, vendors, and use cases for cybersecurity risks**: AI use cases that are associated with core business functions, that carry substantial regulatory risks, or that are widely implemented across the firm may be considered higher risk and should be considered for special cybersecurity and regulatory compliance review.

To subscribe to the Data Blog, please click here.

* * *

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
jlrobins@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

Cameron Sharp
Associate, New York
+ 1 212 909 6673
cdsharp@debevoise.com

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

Mengyi Xu
Associate, San Franciksco
1 415 738 5725
mxu@debevoise.com