



November 21, 2024 | 10 minute read

Welcome to the latest issue of Bracewell's FINRA Facts and Trends, a monthly newsletter devoted to condensing and digesting recent FINRA developments in the areas of enforcement, regulation and dispute resolution. This month, we report on FINRA's comprehensive report on the growing impact of the metaverse on financial firms' regulatory obligations, new cybersecurity risks flagged by FINRA, FINRA's findings related to the recommendation of complex trading strategies to customers, compliance with Form CRS, and much more.

FINRA Publishes Metaverse Report

FINRA has released a [report](#) examining the potential risks and regulatory challenges the metaverse poses to the financial industry. This report is part of FINRA's ongoing efforts to ensure that broker-dealers remain compliant with existing laws and regulations as new technologies like virtual and augmented reality spaces, including the metaverse, gain prominence. FINRA appears intent on making this a long-term objective and has characterized this report as "an initial step in beginning an important dialogue with market participants about potential use of the metaverse within the securities industry."

The report highlights several key findings and considerations for financial institutions and investment firms in relation to the evolving metaverse, including:

- **New Opportunities and Risks:** The metaverse presents a new frontier for financial services, offering novel ways for investors to engage, trade, and interact in virtual environments. However, this also brings new risks related to fraud, money laundering, and the potential for manipulation of virtual financial markets. As the metaverse allows for more immersive and digital financial

Related People

Joshua
Partner
NEW YORK
+1.212.508.6153
joshua.klein@bracewell.com

Russell
Senior Counsel
NEW YORK
+1.212.508.6149
russell.gallaro@bracewell.com

Related Industries

[Finance](#)

Related Practices

[Government Enforcement & Investigations](#)
[Litigation](#)
[Financial Institutions](#)

activities, regulatory authorities must consider how traditional financial rules apply to these virtual spaces.

- **Consumer Protection and Compliance:** The report stresses the importance of maintaining strong consumer protection in virtual spaces. Since financial services in the metaverse will likely be conducted through virtual assets, such as cryptocurrency, or through digital representations of real-world products, FINRA is concerned about the possibility of consumer harm resulting from misrepresentation or lack of transparency. Financial firms must ensure that their marketing, sales practices, and compliance with existing regulations carry over seamlessly into these new virtual environments.
- **Data Privacy and Security:** One of the central challenges of financial activities in the metaverse is the handling of personal data and sensitive financial information. Virtual interactions, often involving avatars or anonymous profiles, complicate the collection and management of client data. The report underscores the need for firms to apply existing privacy and cybersecurity frameworks to the metaverse, while also adapting them to the unique risks of virtual environments, such as hacking, data breaches, or identity theft.
- **Regulatory Oversight:** FINRA acknowledges that the current regulatory framework was designed with traditional financial markets in mind and does not fully account for the complexities introduced by virtual worlds. The report notes the need for updated regulations that are tailored to the metaverse's distinctive features. This includes clarifying whether existing rules governing areas like securities trading, asset management, and investment advice apply to metaverse transactions. Firms will need to evaluate whether their compliance programs need to be updated to address issues like virtual currencies and digital asset management.
- **Future Regulation and Industry Engagement:** FINRA's report indicates that it will continue to monitor developments in the metaverse and engage with stakeholders across the industry, including financial institutions, technology providers, and other regulators. This will help ensure that financial activities in the metaverse are safe, secure, and in line with existing standards. FINRA is open to working with industry participants to refine existing laws and provide additional guidance as the space continues to evolve.

The report calls for increased awareness and proactive action from financial firms, urging them to be vigilant about the risks associated with the metaverse. While the metaverse presents opportunities for financial innovation, companies must ensure that their operations in virtual environments adhere to legal and regulatory standards. This includes upholding consumer protection, ensuring privacy and security, and maintaining proper oversight of virtual financial transactions.

As the metaverse continues to expand, financial institutions and regulators will need to collaborate closely to adapt to its challenges and opportunities. FINRA's report is an important first step in addressing how the metaverse will intersect with traditional finance and regulatory frameworks in the years to come.

FINRA Highlights Increasing Cybersecurity Risks at Third-Party Providers

FINRA's Cyber and Analytics Unit (CAU) has issued an advisory emphasizing the growing cybersecurity risks associated with third-party service providers in the financial services industry. This advisory highlights the increasing reliance on external vendors for critical services and the potential vulnerabilities these third parties introduce to financial firms' cybersecurity frameworks. As the industry becomes more dependent on third-party providers, FINRA urges firms to reassess and strengthen their cybersecurity measures to address emerging risks.

Key Takeaways From the FINRA Advisory

- **Rising Cybersecurity Threats From Third-Party Providers:** FINRA's report underscores that third-party service providers, including cloud service vendors, data processors, and IT infrastructure providers, have become integral to financial firms' operations. However, these external vendors also expose firms to new cybersecurity risks, as they can be potential entry points for cyberattacks. The risks range from data breaches and system outages to more advanced threats such as ransomware and supply chain attacks, which could significantly disrupt business continuity. The alert points to several high-profile cybersecurity incidents where third-party vulnerabilities were exploited, compromising the integrity and confidentiality of client data. With financial firms increasingly outsourcing sensitive operations such as data storage and transaction processing, the scope of potential damage from a cyberattack on a vendor has become a major concern.
- **Regulatory Expectations for Cybersecurity Oversight:** FINRA stresses that firms are ultimately responsible for ensuring the security of their operations, including the cybersecurity practices of their third-party providers. Financial firms must adopt a robust vendor risk management framework that incorporates cybersecurity risk assessments for all third-party relationships, particularly those involving access to sensitive or critical data. This includes ensuring that third-party service providers adhere to appropriate security standards, comply with relevant data protection regulations, and implement comprehensive incident response protocols. FINRA also notes that firms should conduct due diligence when selecting third-party vendors, continually

monitor third parties' performance, and regularly update their security practices in response to emerging threats. As part of their responsibility, firms must assess the cybersecurity controls of these vendors and require them to maintain specific security certifications and safeguards.

- **Third-Party Risk Assessment and Monitoring:** One of FINRA's key recommendations is for firms to have a structured approach to third-party risk assessments. This includes evaluating the cybersecurity posture of potential vendors *before* entering into relationships, as well as ongoing monitoring once the relationship is established. FINRA encourages firms to establish clear contractual obligations with vendors regarding cybersecurity measures, including access controls, data encryption, and disaster recovery plans. Moreover, firms should require their third-party providers to notify them of any cybersecurity incidents, including potential data breaches or attacks that may affect the firm's operations or client data. The report stresses that monitoring should not be a one-time exercise but an ongoing part of a firm's broader cyber risk management strategy.
- **Practical Steps for Firms:** FINRA offers practical guidance for firms to mitigate cybersecurity risks associated with third-party vendors. Key steps suggested by FINRA include:
 - Conducting thorough due diligence before selecting third-party service providers, ensuring they have a strong cybersecurity framework.
 - Requiring third-party providers to adhere to security best practices and provide regular updates on their cybersecurity measures.
 - Establishing contractual provisions that mandate that the third party maintain certain security standards and report any breaches or incidents promptly.
 - Implementing continuous monitoring of third-party cybersecurity practices and integrating them into the firm's overall risk management strategy.
 - Training staff on third-party cybersecurity risks to ensure they are aware of potential threats and know how to respond appropriately.

FINRA's message is clear: financial firms must be proactive in addressing cybersecurity risks, particularly those introduced by third-party providers. With the increasing digitalization of financial services and the growing complexity of vendor relationships, ensuring that third-party vendors adhere to robust cybersecurity standards is vital to safeguarding sensitive data and maintaining the integrity of financial systems. It is crucial for firms to adopt a comprehensive third-party risk management strategy to protect their clients and safeguard the financial system.

Notable Enforcement Matters and Disciplinary Actions

- **Failure to Report Customer Complaints.** FINRA censured a financial services company and its retail brokerage firm, and fined them collectively more than \$1.8 million, for failure to timely report customer complaints and failure to supervise mutual fund purchases.

According to FINRA, the firm failed to report any customer complaints via FINRA Rule 4530 filings and amendments to Forms U4 and U5, from at least January 2018 through September 2021, despite receiving approximately 450 customer complaints during this period. When the firm eventually did disclose many of those complaints in 2023, the disclosures were, on average, over three years late. FINRA further alleged that the firm failed to establish reasonable controls to promptly research complaints, and relay determinations about the reportability of customer complaints to the personnel responsible for making the necessary Form U4 and U5 amendments.

Additionally, for the period from January 2012 through at least December 2017, FINRA alleged that the firm failed to reasonably supervise at least 700,000 direct mutual fund purchases, and failed to configure the firms' automated surveillance systems to review certain types of direct business transactions. According to FINRA, these failures resulted in customers incurring approximately \$111,000 in excessive sales charges and commissions.

FINRA further noted that the firm self-reported its failure to supervise direct business transactions, and conducted its own comprehensive retrospective review.

- **Retail Communications.** A broker-dealer agreed to a censure and a \$40,000 fine related to retail communications related for private placement investments that did not meet the content standards in FINRA Rule 2210.

The specific retail communications that were the target of FINRA's allegations were two emails, which discussed potential investment opportunities related to pre-IPO stage companies, and which linked to news articles regarding those companies. According to FINRA, these emails were not "fair and balanced" because they did not prominently disclose the risks associated with the potential investments. Similarly, FINRA also alleged that the company approved a slide deck that discussed private placements generally, which failed to prominently disclose that such securities are

speculative, illiquid, and carry a high degree of risk.

Separately, the same firm also failed (according to FINRA) to timely file with FINRA offering documents related to 92 private placement investments. FINRA alleged that, on average, the firm's filing of these offering documents were 163 days late, or 178 days after the first sale of the offerings.

Inadequate Real Estate Investment Due Diligence. FINRA has ordered a broker-dealer to pay \$800,000 in restitution and penalties to resolve claims related to improper investment recommendations. FINRA alleged that the firm failed to satisfy its reasonable basis suitability obligation, in violation of FINRA Rules 2111 and 2110, by allegedly recommending real estate-focused private placements without conducting adequate due diligence, which led to investor losses when the investments failed.

According to FINRA's findings of fact, the firm acted as a placement agent for three private offerings — and between June 2017 and February 2018, the firm did not conduct reasonable due diligence for the offerings, which the firm recommended to its customers. In addition, FINRA stated that the firm violated its own written supervisory procedures by not establishing a proper committee to review new products before offering them to clients. The marketing materials provided by the real estate company to the firm only contained limited financial information about the projects, preventing the firm from fully assessing the risks and potential returns. When the real estate company and its affiliates filed for bankruptcy in March 2021, investors who had purchased the securities were harmed. FINRA criticized the firm for failing to obtain sufficient financial details to understand the project's capital structures or evaluate the risks involved.

The firm was also cited for other violations over a seven-year period, including distributing inaccurate trade confirmations and failing to identify non-legitimate trades. From March 2020 to October 2021, FINRA alleged that the firm lacked tools to detect suspicious trading activity. Additionally, the firm mistakenly reported over 3,400 customer transactions from January 2021 to December 2023 to FINRA's Trade Reporting and Compliance Engine.

Complex Trading Strategies. A Georgia-based brokerage firm has agreed to pay \$2 million in partial restitution to resolve claims made by FINRA. The allegations center around the firm's recommendation of a high-risk trading strategy to over 350 customers without fully understanding the strategy's features and risks.

FINRA found that, between July 2014 and February 2018, the firm recommended a trading approach that involved primarily exchange-traded

notes (ETNs) linked to volatility. This strategy was designed to generate returns when volatility decreased. However, FINRA stated that the ETN was complex, high-risk, and meant for short-term holding — something the firm failed to properly understand and communicate to clients, in violation of FINRA Rules 3110 and 2010.

Despite warnings in the ETN's disclosure documents, which noted the potential for significant losses during market volatility, the firm and its president kept customers invested in the ETN for long periods, including during a surge in volatility in February 2018. This led to nearly total losses for those customers when the ETN's value plummeted.

FINRA also criticized the firm's inadequate testing of the strategy, using incomplete data that overestimated its potential returns, which led to a misunderstanding of the risk/reward profile. According to FINRA, the firm had no procedures in place to assess the suitability of the strategy for individual clients, nor did it analyze the concentration of customer investments in the ETN.

In addition to the \$2 million restitution figure, the firm received a censure and its president faced a \$15,000 fine and a six-month suspension from FINRA.

Ignoring Information Requests. A New York-based brokerage firm has been fined \$115,000 by FINRA for a series of regulatory violations. These violations, detailed [here](#), stem from the firm's noncompliance with various FINRA rules, specifically Rule 8210, which requires firms to comply with requests from FINRA for documents or information necessary to investigate possible violations. Between June 2021 and August 2023, FINRA alleged the firm failed to timely respond to three requests made pursuant to FINRA Rule 8210, and did not fully comply with these three requests until after FINRA issued four follow-up FINRA Rule 8210 requests and pursued three expedited proceedings to compel its compliance, in violation of FINRA Rules 8210 and 2010. The firm also failed to reasonably supervise its compliance with FINRA Rule 8210 by not having a reasonable system to track deadlines for Rule 8210 requests and not adequately staffing its compliance department or training its existing staff to respond to Rule 8210 requests. Finally, the firm failed to take reasonable measures to improve its supervision system, despite facing three expedited proceedings for failing to respond to Rule 8210 requests in less than two years. As a result, the firm violated FINRA Rules 3110(a) and 2010.

In addition to the financial penalty, the firm was also required to improve its compliance practices and bolster its supervisory framework to ensure that future violations do not occur. The settlement also includes additional provisions to strengthen the firm's internal controls, including a requirement

for the firm to enhance its review of transactions involving customer accounts and improve its internal reporting systems to detect potential violations earlier.

FINRA's decision is part of its broader enforcement efforts to hold broker-dealers accountable for failures in supervisory and compliance practices. The fine serves as a warning to other firms in the industry about the importance of maintaining adequate supervision and adhering to regulatory requirements to safeguard investor interests.

Failure to Disclose Disciplinary History on Form CRS. On November 11, FINRA censured and fined a brokerage firm \$30,000 for failing to disclose the firm's complete legal and disciplinary history on its Form CRS.

According to FINRA, between June 30, 2020 and May 1, 2023, the firm did not meet the necessary obligations under the SEC's Regulation BI, which mandates that firms deliver Form CRS to retail customers. The firm and four of its control affiliates had prior reportable legal or disciplinary history. "However, [the firm] did not respond 'Yes' or direct retail investors to Investor.gov/CRS in response to the question concerning legal or disciplinary history on the Form CRS it filed on June 30, 2020, or on its amended Form CRS filed on April 14, 2022," FINRA's findings of fact state. On May 1, 2023, "the firm filed an amended Form CRS that responded 'Yes' to the question concerning legal or disciplinary history and directed retail investors to Investor.gov/CRS."

FINRA has been keenly focused on firms' compliance with Form CRS, which is designed to provide retail investors with important information about a firm's services, fees, conflicts of interest, and whether the firm acts as a broker-dealer or an investment adviser. The firm's failure to provide an accurate form to its customers violated the rules aimed at increasing transparency and ensuring that investors are fully informed. As part of the settlement, the firm agreed to take corrective actions, including reviewing and revising its policies and procedures related to Form CRS delivery and filing, as well as other compliance measures to prevent future failures.

This disciplinary action underscores the critical importance of adhering to FINRA and SEC regulations regarding investor disclosures and transparency. Firms must be diligent in their responsibilities to ensure that customers are provided with the necessary documents to make informed decisions, including Form CRS, and that these documents are filed properly with regulators like FINRA.