THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 57 No. 20 November 20, 2024

FRAUD IN THE TECHNOLOGY AGE: STRATEGIES FOR DETECTION, PREVENTION, AND NAVIGATING REGULATORY INQUIRIES

In this article, the authors provide an overview of common frauds in the financial services industry. They then turn to best practices for preventing and detecting fraud, regulatory compliance requirements, and discuss recent enforcement actions related to the responsibilities of regulated entities. They conclude with best practices for avoiding and managing regulatory scrutiny through a comprehensive approach.

By Jan M. Folena and Samantha B. Kats *

In today's complex and technology-driven financial landscape, the threat of fraudulent acts and practices that harm investors and the financial institutions that serve them is significant.[1] It is estimated that over $50 billion per year is lost to fraud.[2] Data shows that fraud has had a surprisingly proportionate impact across various age groups with varying degrees of investor sophistication.[3] While the fraud itself can have a devasting impact on investors, firms should be aware of the regulatory scrutiny that can result from fraudulent acts, whether they originate from inside the firm or from outside actors.

State-of-the-art technology and tools allow scammers to tap into trustworthy sources and fool even the most sophisticated network systems. Similarly, firm

[1] AARP Fraud Watch Network, FINRA Investor Education Foundation, and Heart+Mind Strategies, *Blame and Shame in the Context of Financial Fraud*, June 2022.

[2] Christine Kieffer, *Victim Blaming Harms Us All*, FINRA Office of Investor Education, Mar. 6, 2024 (referencing FINRA Investor Education Foundation research report, *Non-Traditional Costs of Financial Fraud*).

[3] Federal Trade Commission, Consumer Sentinel Network, *Data Book 2023*, Feb. 2024, at 13, (showing that individuals between the ages of 30 to 39 and 60 to 69 are equally impacted and comprise a total of 36% of all reported frauds totaling $1.82 billion in losses).

* *JAN M. FOLENA is a partner at Stradley Ronon Stevens & Young LLP in Washington, D.C. As co-chair of the firm's securities enforcement practice, she advises and represents clients in financial regulatory enforcement matters involving federal securities laws and associated rules and regulations. SAMANTHA B. KATS is managing counsel in the firm's Malvern, Pennsylvania, office. She focuses her practice on securities litigation, internal investigations, regulatory actions, complex civil litigation and fiduciary litigation, representing corporate, nonprofit, financial services industry, and institutional clients. Their e-mail addresses are jfolena@stradley.com and skats@stradley.com.*

RSCR Publications LLC Published 22 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $1,197 per year in U.S., Canada, and Mexico; $1,262 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call 609-683-4450; fax 609-683-7291; write Subscriber Services, RSCR Publications, PO Box 585, Kingston NJ 08528; e-mail cri.customer.service@comcast.net; or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 0884-2426.

technology in place to increase efficiency and assist investors is not infallible. Even with the best of intentions, fraud occurs and could subject firms to civil liability as well as regulatory scrutiny. Financial services firms can protect investors and themselves by ensuring adequate policies and procedures, and internal controls are in place to prevent and detect fraud early and implement plans to manage fraud if it occurs.

COMMON FRAUDS

Fraud has many forms, each representing unique challenges for detection and prevention. Investors may be victimized by scams that originate outside of the firm, such as a hack into a firm's network systems or a cybersecurity breach that exposes sensitive personal and financial information. When firm technology, systems, and/or controls are not functioning properly to monitor and detect fraudulent practices, it creates weaknesses that scammers can exploit. Similarly, rogue brokers, agents, and employees may abuse their positions of trust. Further, an internal failure of the firm's technology systems in place to assist, among other things, in trading and managing accounts may operate as a fraud on investors. Considering the variety and complexity of potential fraudulent practices, it is imperative to implement robust preventative measures to safeguard against such threats and control the potential regulatory risk they may cause.

PREVENTION THROUGH EDUCATION, INTERNAL CONTROLS, AND PROCEDURES

Research shows that recurring education about investment fraud can reduce receptiveness to fraud by helping individuals recognize, avoid, and report suspected fraudulent acts.[4] The good news is that there are countless resources available that can be implemented to educate firm employees and investors at the click of a button. These include, but are not limited to, investor education websites offered by the U.S. Securities and Exchange Commission ("SEC"), Securities Industry and Financial Markets Association ("SIFMA"), North American Securities Administrators Association ("NASAA"), and the American Association of Retired Persos ("AARP").[5] In addition to offering frequent training and identifying educational resources, it is equally important to consistently evaluate and test your network systems and internal controls to ensure technology is functioning properly and has not been and cannot easily be overridden.

Do not wait for an issue to arise to learn that there is a gap in the firm's internal controls, or a network system is malfunctioning. It is better to catch a problem days after it happens rather than months or years later when the effects may be devastating. Policies and procedures should detail the systems and controls in place and undergo periodic testing, which should be documented in the normal course. If the firm or its clients are the target of investment fraud or a cyberattack, regulators are likely to inquire about and examine the firm's policies and procedures and whether the firm complied with them, the supervision and testing of internal systems and controls for preventing and detecting fraud, and the overall response to the incident.

FRAUD MAY INVITE REGULATORY SCRUTINY

Recent regulatory examination and enforcement priorities, specialized enforcement units, enforcement sweeps, and enforcement actions emphasize the potential for serious consequences regarding fraud within the securities industry. The SEC and Financial Industry Regulatory Authority ("FINRA") have increased focus on areas such as cybersecurity, financial technology, and artificial intelligence ("AI"). Since 2017, the SEC has boasted a cybersecurity unit within the Division of Enforcement and has included information security, operational resiliency, and emerging financial technology on its 2022, 2023, and 2024 exam priorities. Exam and enforcement priorities often overlap and, at the very least, a failure of or deficiency in information security or financial technology identified by a regulator

[4] Angelita Williams, *New Research: Repeated Exposure to Fraud Awareness Education Reduces Susceptibility to Investment Scams,* Mar. 10, 2021.

[5] SEC, Investor Education; SIFMA, Senior Investor Protection Toolkit; NASAA; AARP Fraud Watch Network.

during an exam can lead to an enforcement inquiry. In recent years, certain regulatory enforcement inquiries and actions have focused on firms' preparation for and response to fraudulent activities and their use and implementation of financial technology.

Responding to Fraud: Compliance with Reporting Requirements

FINRA recently made clear the importance of following reporting requirements when allegations of fraud are made by customers or an actual fraud occurs involving investors at a registered firm. In November 2023, FINRA filed an action against a member firm for failing to promptly report written customer complaints involving allegations of theft or misappropriation of funds or securities and failing to report certain settled matters in violation of FINRA Rules 4530, 3110, and 2010.[6] FINRA concluded that the member firm failed to enforce its written supervisory procedures for the reporting of customer complaints pursuant to FINRA Rule 4530(a)(1)(B) and to establish or maintain a supervisory system, including written supervisory procedures, reasonably designed to achieve compliance with FINRA reporting requirements pursuant to FINRA Rule 4530(a)(1)(G).[7]

While FINRA did not hold the firm responsible for any involvement in the fraudulent activities, the regulator sanctioned the firm for its failure to establish and maintain an appropriate supervisory system, including written supervisory procedures, that were reasonably designed to achieve compliance with FINRA reporting requirements. The action serves as a reminder and incentive to firms to ensure systems are in place to not just detect and prevent fraudulent activity but to ensure that all regulatory reporting obligations are met.

Regulatory Focus on Cybersecurity Disclosures

Cybersecurity is an area that the SEC continues to prioritize in relation to the agency's investor protection mandate. The SEC's Crypto Assets and Cyber Unit focuses on addressing the growing threat of cyberattacks and breaches in the financial industry and ensuring that financial institutions adhere to proper protocols to protect clients' personal information and mitigate cybersecurity lapses that may lead to investor losses. The SEC has promulgated cybersecurity rules applicable to public companies to ensure that cybersecurity incidents are fully disclosed and managed, although it has delayed implementation of similar rules applicable to investment advisers, registered investment companies, and business development companies.[8] Simultaneously, the SEC has been reviewing compliance with the federal securities laws when public companies experience a cybersecurity incident.

Even the most robust security measures sometimes fail, leaving public companies and firms vulnerable to cyberattacks. Beyond the immediate impact on operations and financial harm, such incidents can also attract regulatory scrutiny, leading to legal consequences, fines, and reputational damage. For example, in May 2020, the SEC charged public company First American Financial Corp., one of the largest providers of title insurance and settlement services, for failing to implement sufficient disclosure controls and procedures to ensure that information required to be disclosed following a cybersecurity incident is timely recorded, processed, and summarized.[9]

The enforcement action followed a significant data breach that exposed more than 800 million sensitive document images that contained Social Security numbers, bank account numbers, wire transaction receipts, and driver's license images. The SEC's investigation found that First American's cybersecurity vulnerability stemmed from a known security flaw in its document sharing system that the company discovered in January 2019. Although First American filed a Form 8-K with the SEC on May 28, 2019, within days of learning of the cybersecurity breach, the SEC alleged that First American's statement in the Form 8-K that it had "no preliminary indication of large-scale unauthorized access to customer information" was false. According to the SEC, when the company became aware of the flaw in its document-sharing system in January, it failed to convey the information to the senior executives responsible for the disclosures. As a result of this oversight, First American faced an SEC enforcement action in which the firm agreed to pay a civil penalty of $487,616.

In October 2023, the SEC filed a litigated enforcement action against software company SolarWinds Corp. and its chief information security

[6] FINRA Rules 4530, 3110 and 2010.

[7] FINRA Rule 4530(a)(1)(B) and (G).

[8] Proposed Rule 206(4)-9 under the Investment Advisers Act of 1940 and Proposed Rule 38a-2 under the Investment Company Act of 1940.

[9] *In the Matter of First American Financial*, Rel No. 92176 (June 14, 2021).

officer ("CISO"), who was at the relevant time the company's vice president of security and architecture. The SEC cited the defendants for failing to accurately describe the firm's known cybersecurity risks and vulnerabilities prior to and after a significant cyberattack that compromised its products and the customers using the products.[10] According to the SEC, SolarWinds misled investors by disclosing only general and hypothetical risks to the company when it was well aware that it was unable to protect the company from cyberattacks. The matter is a rare, litigated action against a public company, but demonstrates the SEC's focus on effective cybersecurity management and accurate disclosures. The regulator sought an injunction, disgorgement, civil penalties, and an officer and director bar against the now-CISO. On July 18, 2024, the U.S. District Court for the Southern District of New York dismissed most of the SEC's claims against SolarWinds and its CISO.

This case demonstrates how an outside threat can exploit internal weaknesses, and not only compromise the company but also its customers by embedding malicious code into company products used by customers. If the known security vulnerabilities had been disclosed and addressed earlier, the effects of the fraud could have been mitigated and a regulatory enforcement action may have been prevented.

The cyberattack against Washington-based law firm Covington & Burling in November 2020 marked a significant breach that not only compromised the firm's sensitive data, but also led to a high-profile investigation and subpoena enforcement action by the SEC. The attack, which targeted Covington's confidential information, raised concerns regarding potential insider trading based on material nonpublic information obtained through unauthorized means and about whether the law firm's public company clients had failed to report or misreported the impact of the cyberattack on their businesses.[11] These concerns led the SEC to issue a controversial investigatory subpoena to Covington seeking, among other things, the names of the firm's public company clients impacted by the attack and any communications that Covington provided to each client regarding the attack. The law firm raised objections based on attorney-client privilege and confidentiality grounds.[12] The court ultimately ordered Covington to comply with a modified SEC request by providing only the names of seven of its 300 impacted clients.[13]

This subpoena enforcement action underscores the evolving threat surrounding cybersecurity breaches within the legal and financial industries and the regulatory scrutiny faced by firms implicated in such incidents. The Covington cyberattack and its aftermath serve as a stark reminder of the importance of robust cybersecurity measures to safeguard against cyber threats and thorough policies and procedures to manage the misappropriation of nonpublic information, regulatory reporting obligations, and prompt remediation.

Conduct That Operates as a Fraud

The idea that the mere use of financial technology may result in a regulatory enforcement action seems unusual, but recent examples from the SEC may indicate a trend. The anti-fraud provisions of the Securities Act of 1933 and the Investment Advisers Act of 1940 ("IAA") include non-scienter or negligence-based violations that prohibit conduct that "operates as a fraud" on investors. This year, the SEC instituted enforcement actions against two robo-adviser firms, Delphia (USA) Inc. and Global Predictions Inc., for violations of Section 206(2) of the IAA resulting from false and misleading representations about the capabilities of their AI and machine-driven investment strategies and further sanctioned the firms for general oversight failures.[14]

The SEC alleged that Delphia made misleading statements regarding the inputs used in its AI or machine learning investment strategies and that its algorithms were not capable of incorporating client data into its investment recommendations as advertised. According to the SEC, these technology deficiencies caused the firm's representations related to the firm's use of AI to be misleading and, thus, operated as a fraud on investors. In addition, the firm allegedly failed to adopt and implement policies to ensure that statements made to investors were accurate; i.e., consistent with the firm's technological capabilities. In settling the charges, Delphia agreed to pay a civil penalty of $225,000.

---

[10] *SEC v. SolarWinds*, 23-Cv-9518 (S.D.N.Y. Oct. 30, 2023); SEC Press Release, *SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures*, Oct. 30, 2023.

[11] *SEC v. Covington & Burling*, 23-mc-00002 (D.D.C 2023).

[12] *Id*.

[13] *Id*.

[14] *In the Matter of Delphia (USA)*, Rel. No. 6573 (Mar. 18, 2024); *In the Matter of Global Predictions*, Rel. No. 6574 (Mar. 18, 2024).

The SEC charged Global Predictions for similar violations relating to misleading representations about its AI-based investment strategies. According to the SEC, Global Predictions misrepresented the functionality of a chatbot and falsely claimed that its algorithms, which appear to have existed, incorporated expert AI-driven forecasts. The SEC alleged that these technology deficiencies operated as a fraud on investors. Global Predictions settled the charges by agreeing to a civil penalty in the amount of $175,000.

These recent cases are not the first time that the SEC has brought charges related to disclosures regarding the use and implementation of firm technology. An early example of similar charges by the SEC concerning inadequate and misleading disclosures in connection with the use of an algorithmic trading system is the SEC's enforcement action against United Kingdom-based investment adviser BlueCrest Capital Management Ltd.[15] The SEC alleged that BlueCrest misled investors by not fully disclosing conflicts of interest related to its allocation of live traders from its client hedge fund to its proprietary fund and replacing the live traders with a "semi-systematic, algorithmic trading program" that was intended to replicate the trading performance of the live traders. According to the SEC, BlueCrest knew that the algorithm underperformed the live traders and experienced continuing performance issues yet continued to use the system to execute trades for its client hedge fund.

The SEC alleged that BlueCrest's generic disclosures in Forms ADV and prospectuses failed to adequately disclose the specific details of the algorithm-driven system and the conflicts of interest it created. Ultimately, these failures operated as a fraud upon the adviser's hedge fund clients. The case settled in December 2020, and BlueCrest agreed to pay disgorgement of $107.6 million, prejudgment interest of $25.2 million, and a civil penalty of $37.3 million totaling $170 million.

These cases highlight the growing regulatory scrutiny surrounding the use of advanced technologies in investment strategies and underscore the importance of diligent monitoring of such systems to ensure awareness of any malfunctions, changes in performance, or conflicts of interest that may exist or develop so that required disclosures remain up to date and accurate.

AVOIDING AND MANAGING REGULATORY SCRUTINY

Safeguarding against fraud and managing regulatory scrutiny requires a comprehensive approach that involves technology, robust policies and procedures, internal controls, regulatory compliance, and ongoing education and training. Ensuring that the appropriate procedures are in place to detect and respond to fraudulent activity and to prevent unintentionally misleading investors is essential. Firms should consistently evaluate their policies and procedures relating to preventing, detecting, responding to, and reporting fraud, and consider and document whether they are being effectively implemented and supervised.

Timely detection of fraudulent activity, prompt remediation, and accurate reporting can significantly mitigate, if not avoid, regulatory action. Consistent testing and auditing of technology systems, as well as documentation of such procedures, can also help. Identifying a fraudulent act, cybersecurity incident, or a technology failure early can assist in establishing that the firm's procedures were sufficient and served their intended purpose. Finally, a team of lawyers with regulatory and enforcement experience can be helpful in many ways, including managing and responding to regulatory examinations, inquiries, and investigations; conducting thorough reviews of policies and procedures; assisting with audits of systems; identifying any weaknesses; suggesting improvements; ensuring proper documentation and notification; and offering training. ■

[15] *In the Matter of BlueCrest Capital Management,* Rel. No. 10896 (Dec. 8, 2020).