

Navigating the Future: Key Takeaways & Insights from the 2024 Securities Enforcement Forum Central

During the Securities Enforcement Forum Central hosted by Securities Docket in Chicago, professionals across the private and public sectors participated in a series of panels covering many of the recent developments in the securities enforcement field. Below is a summary of Alexander Cohen and Emily Fulginiti's key takeaways and insights that every SEC registrant should review.

Post-Jarkesy Collateral Attacks

One of the concerns following the Supreme Court's ruling in *SEC v. Jarkesy* was that other agencies may face similar collateral attacks to its administrative proceedings. While the full impact of *Jarkesy* remains an open question, the *Jarkesy*-esque challenge has already been asserted in connection with a FINRA proceeding.¹ In that case, the Court rejected the collateral attack by punting on the question of whether the underlying action was properly brought before a FINRA forum. The Court dismissed the respondent's arguments based upon a lack of subject matter jurisdiction and allowed the FINRA action to proceed through its administrative process. Defendants are carefully considering today whether they should pursue some form of injunctive relief in response to a securities administrative action in light of *Jarkesy* as well as other favorable Supreme Court rulings such as *SEC v. Lucia* and *SEC v. Cochran* that provide further avenues to challenge the constitutionality of an administrative proceeding. As the appetite to raise these constitutionality concerns continues to grow among the defense bar, we should expect to see more actions filed by the SEC in federal court.

Cooperation Credit and Self Reporting

Cooperation credit and self-reporting have been topics of heavy interest for the SEC over the past twelve months. The SEC's former Enforcement Director offered helpful guidance on the key principles of effective cooperation in a speech delivered earlier this year. In addition, recent settlement orders have become a great tool for the agency to further address many of the common questions within the industry, such as:

1. what kind of conduct is expected to earn cooperation credit, and
2. what are the ultimate benefits of cooperation.

As an example, on September 23, 2024, the SEC announced yet another off-channel communications settlement for recordkeeping violations with a registered investment adviser who discovered its books and records violations in the course of responding to an agency subpoena in an unrelated matter. The SEC acknowledged that the final resolution did not impose a penalty against the firm because it self-reported,² promptly remediated, and provided substantial cooperation in various other ways. Indeed, we have recently seen firms engage in similar forms of cooperation in the context of recordkeeping and non-recordkeeping matters and, accordingly, receive benefits based on their efforts.³ If a firm is considering self-reporting to the SEC, it must also not disregard its reporting obligations to FINRA triggered under Rule 4530 as well as the related practical considerations that come with notifying a major securities regulator. Regardless of whether a firm self-reports, it's still critical to diligently document the investigation and findings in the event that a regulator approaches the firm later on about the issue.

Insider Trading Enforcement Updates



Alexander I. Cohen

Member

aicohen@cozen.com
Phone: (212) 453-3778
Fax: (212) 509-9492



Emily M. Fulginiti

Associate

efulginiti@cozen.com
Phone: (212) 453-3974
Fax: (212) 509-9492

Related Practice Areas

- Securities Litigation & SEC Enforcement

Despite substantial investments in surveillance, insider trading is widespread in the market and at times difficult to detect for both FINRA and the SEC. However, when it is discovered, the Commission will prosecute even the small dollar cases in furtherance of promoting its goal of general deterrence in the marketplace. Where appropriate, the Commission has demonstrated that it will pursue new theories of liability for insider trading when a novel trading scenario emerges that is not covered by existing precedent. The SEC will seek to establish the necessary elements of an insider trading claim by considering multiple sources of evidence. For example, a company's insider trading policy, an employee's Non-Disclosure Agreement, and the general duties of the common law could all play an important role in establishing an individual's duty of confidentiality. As a result, companies can help mitigate and manage risk by considering whether their existing insider trading policies and other collateral agreements are keeping pace with the SEC's expanded views of liability. Another category of evidence is off-channel communications – an area that has clearly garnered significant regulatory attention over the past few years and should be expected to become a common item on the list of the government's requests in these cases. This additional source of evidence could prove pivotal in establishing other core elements of the claim, such as possession of the MNPI or the requisite state of mind.

SEC's Cyber and Recordkeeping Enforcement Raises the Bar on Compliance Standards

Over the last year, the industry has responded with considerable pushback in response to the SEC's use of the internal accounting controls provision of the Foreign Corrupt Practice Act (the internal controls provision)⁴ to pursue public companies that are the victim of a cybersecurity incident. The SEC has not only promulgated new rules requiring public companies to disclose material cybersecurity incidents but just a few months ago, the SEC brought a settled enforcement action for the first time against a public company for violating the internal controls provision by failing to maintain adequate cybersecurity controls that reasonably protected against the unauthorized access of its information technology systems and networks.

This was a monumental step in enforcement for two reasons that were well articulated by two Commissioners at the agency. First, the SEC sought to expand the application of a rule designed to enhance the accuracy and completeness of an issuer's financial reporting by using it to challenge a company's cybersecurity defenses and practices.⁵ And second, the SEC's groundbreaking precedent has potentially opened the floodgates for any cybersecurity incident to become the subject of an enforcement action.⁶ Specifically, the standard of liability set forth by the agency in this recent action has stoked major concerns of whether the internal controls provision has suddenly become a hammer to pursue a compliance standard of perfection as opposed to reasonableness. If it's not already complicated enough, the regulatory landscape has since become more muddled after a court in the Southern District of New York rejected in separate litigation the SEC's same application of the internal controls provision to a company's cybersecurity activities.⁷ The industry is left to wonder how the agency will respond to future cybersecurity incidents and, specifically, which future intrusions, if any, will warrant enforcement actions under the internal controls provision.

Interestingly, the agency's official statements issued after the rule's adoption several decades ago acknowledged that a company's accounting control systems occasionally fail and that the identification of an isolated breach does not independently constitute a violation of the law.⁸ More recently, the same two SEC Commissioners issued a dissent to an off-channel communications settlement after a more than decade-long effort by the respondent to strengthen its books and records compliance regime.⁹ The final order in that case found that the firm failed to implement "a system reasonably expected to determine whether *all* personnel . . . were following the [firm's] procedures" as well as "implement sufficient monitoring to ensure that its recordkeeping and communications policies and procedures were *always* being followed." When announcing the settled charges, the SEC noted that the firm would not pay a penalty because it self-reported, cooperated, and demonstrated substantial compliance efforts. However, many in the industry were left asking themselves why an enforcement action should have been brought at all in the first place. It's positive to hear some of the Commissioners supporting a pragmatic approach that helps registrants comply with the securities laws without seeking a penalty for every technical violation of the law. Nevertheless, recent enforcement actions in cyber and off-channel communications,

among others, suggest a noticeable shift by the agency towards a more rigorous expectation of compliance.

Investment Adviser Fiduciary Duties

An investment adviser who fails to take reasonable steps to satisfy its fiduciary obligations owed to its customers may be exposed to civil fraud liability. In a recent enforcement action against a dual registrant, the SEC charged the firm with violating Section 206(2) of the Investment Advisers Act (the anti-fraud provision) by failing to provide its customers with full and fair disclosure regarding certain conflicts of interest. Such conflicts were associated with, among other things, the firm's receipt of revenue-sharing payments from its unaffiliated clearing broker as a result of retail clients' investments in certain no-fee mutual funds and money market funds. The order also noted that the firm breached its duty of care by failing to undertake an analysis to determine whether the mutual funds and money market funds were actually in the best interests of its clients. Importantly, the SEC need only demonstrate negligence when establishing that a firm violated the antifraud provision of Section 206(2) (not scienter). There were no allegations by the SEC that the firm made any false or misleading statements to its clients, but the breach of its fiduciary duties was sufficient conduct for the SEC to bring a fraud charge in this case. The firm was ordered to pay disgorgement and prejudgment interest of approximately \$5 million as well as a civil penalty of \$1 million. In addition to these sanctions, the firm was subject to a cease-and-desist order, a censure, and several undertakings that included the obligation to evaluate whether its existing clients should be moved out of their current holdings and into lower-cost investment alternatives. While reasonable minds may differ about whether the SEC should have brought an anti-fraud charge against the IA in the first place, it's an interesting example of prosecutorial discretion to protect the best interests of retail customers.

Looking Ahead

Securities enforcement is on the rise compared to last year, and when it's released, we expect the SEC's annual enforcement results report for this past fiscal year to reflect that reality. Insider trading and the general goal of enhancing public trust in U.S. markets remain a major priority of the Commission, but there are several other areas of interest the agency is focused on across divisions:

1. Investor protection of retail customers.
 - Regulation Best Interest, IA's related fiduciary duties, Marketing Rules, including failure to maintain and enforce policies and procedures reasonably designed to achieve compliance with the relevant rules/obligations.
 - Inadvertent system errors, inadequate policies and procedures, etc., that cause economic harm to customers, including as it relates to new technologies that affect the transactions process (i.e., artificial intelligence, FinTech, and application platforms)
2. Off-channel communications for any registrant with a books and records obligation.
 - Be mindful of FINRA examinations that are now incorporating this issue into their review.
 - If not through an examination, the issue will arise through a subpoena, voluntary request, or even a whistleblower.
 - Review the undertakings in one of the related settlement orders for a remediation roadmap.
3. Gatekeeper liability, including material accounting discrepancies based on a failure to adhere to the auditing standards promulgated by the PCAOB.
4. Crypto asset securities, including ongoing litigation related to fraud schemes, unregistered offerings, platforms, intermediaries, and improper promotion of these assets.
5. Whistleblowers' rights and ability to report potential securities law violations to the government.

¹ *Blankenship v. FINRA*, Case No. 2:24-cv-03003-JFM, 2024 WL 4043442 (E.D. Pa. Sept. 4, 2024).

² As the SEC has explained, “credit” for self-reporting is not available unless the firm is providing information to the agency that it would not otherwise have discovered or which it would not have discovered as quickly.

³ Other examples: Dixon Mitchell and Nationale-Nederlanden were not required to pay civil penalties because they self-reported their violations and otherwise cooperated); A.M. Best and Demotech were not required to retain a compliance consultant because they engaged in significant efforts to comply with the recordkeeping requirements relatively early and otherwise cooperated with the SEC’s investigation.

⁴ Exchange Act Section 13(b)(2)(B)

⁵ The Commissioners’ Statement on R.R. Donnelley & Sons. The Commission, in recent years, has treated the internal controls provision “as a Swiss Army Statute to compel issuers to adopt policies and procedures the Commission believes prudent.”

⁶ *Id.* (“Any departure from what the Commission deems to be appropriate cybersecurity policies could be deemed an internal accounting controls violation. The Commission’s assurances in connection with the recent cyber-disclosure rulemaking ring untrue if the Commission plans to dictate public company cybersecurity practices indirectly using its ever-flexible Section 13(b)(2)(B) tool.”)

⁷ *Securities and Exchange Commission v. SolarWinds Corp.*, Case 1:23-cv-09518 (S.D.N.Y. July 18, 2024) (“[F]ailure to detect a cybersecurity deficiency . . . cannot reasonably be termed an accounting problem.”)

⁸ Speech of Chairman Harold Williams. A fundamental purpose of these rules was to require companies to meet certain reasonableness standards in a manner that is cost-effective, innovative, and works best in light of their unique needs and responsibilities.

⁹ Commissioners’ Statement on Qatalyst Partners LP. The message of the final order is that “even well-intentioned firms could find themselves in the Commission’s enforcement queue time and again.”

Please reach out to Alexander Cohen and Emily Fulginiti with any questions.