JENNER & BLOCK

SEC Priorities Regarding Cybersecurity Enforcement: What Public Companies Need to Know Now in the Second Trump Administration

Client Alerts

March 3, 2025
By: Shoba Pillay, Charles D. Riely, H. Kurt von Moltke, Kathryn Chang, Philip B. Sailer

Introduction

The SEC recently announced the creation of a Cyber and Emerging Technologies Unit (CETU) that will focus on fraudulent conduct in cybersecurity, digital assets, and emerging technologies such as artificial intelligence. For public companies, the announcement indicates that the new unit will focus on combatting fraud and other "cyber-related misconduct," including "public issuer fraudulent disclosure relating to cybersecurity."

The unit's announced focus on "fraudulent" cybersecurity disclosures marks a potential shift from the SEC's recent enforcement approach. This client alert analyzes the SEC's recent announcement in light of the preexisting cybersecurity enforcement landscape and provides key takeaways for public companies.

The SEC's Cybersecurity Enforcement Landscape

The SEC's emphasis on fraudulent conduct likely signals a step back from some of the more aggressive enforcement actions brought during the Biden administration. During the last administration, the SEC repeatedly messaged its high expectations for public companies to analyze, escalate, remediate, and make difficult disclosure decisions about cybersecurity incidents:

- On March 9, 2023, the SEC settled negligence-based charges against a data management company in connection with misleading investors about the scope of a ransomware attack.[1] Over the course of three months, the company initially indicated that the attack had not involved certain information about donors, then learned through its technology and customer personnel that such exfiltration had occurred, and ultimately disclosed the full scope of the attack.[2] The SEC required the company to pay $3 million in penalties[3] despite the relatively short timeframe in which the

company made its initial and revised disclosures regarding the attack and the absence of a finding that the company acted intentionally.

- On June 22, 2023, SEC Enforcement Director Gurbir Grewal warned public companies in a speech to disclose concerns about a data breach to the SEC "sooner rather than later"—even if they only "think [they] might" have a material event to disclose—and regardless of whether the company finished its internal investigation into the incident.[4]

- On July 25, 2023, the SEC adopted new rules for public companies regarding cybersecurity risk management, strategy, governance, and incident reporting (Cybersecurity Rules).

- On October 30, 2023, the SEC filed a high-profile litigation asserting fraud and internal controls charges against software company SolarWinds Corporation and its Chief Information Security Officer, Timothy G. Brown, in connection with the 2020 breach of SolarWinds' network monitoring software system, Orion. This case represented the *first* time the SEC sued a company for *scienter*-based fraud involving disclosures regarding the strength of its cybersecurity practices, as well as its post-incident disclosures; the *first* time the SEC sued a CISO (or any individual) for their role in cybersecurity failures; and the *first* time the SEC sued a company for internal controls failures arising from alleged cybersecurity deficiencies that led to a company's inability to protect its key assets. As detailed below, the SEC suffered a setback when the district court granted a portion of the Defendant's motion to dismiss.

- In May and June 2024, the SEC's Director of Corporation Finance issued guidance regarding how public companies should approach cybersecurity disclosures. This guidance emphasized the SEC's expectations that public companies effectively distinguish material from not-yet material cybersecurity incidents in their disclosures, as well as walk the fine line of discussing an incident with third parties consistent with their overall disclosure obligations.

Significantly, with the exception of the *SolarWinds* litigation, all of the SEC's recent cybersecurity disclosure cases involved company-only settlements where the SEC determined that the companies had reason to know material information about a cybersecurity incident but failed to escalate that information to the individuals within the company making disclosure decisions for the company. In these settlements, the SEC relied on negligence-based fraud under 17(a)(2) and 17(a)(3) of the Securities Act or internal controls charges under the Securities Exchange Act stemming from a company's inadequate policies and procedures regarding the escalation of information regarding a cybersecurity incident. Importantly, Sections 17(a)(2) and (a)(3) do not require scienter—i.e., the intent to deceive—or more, an individual on whom to premise company liability for making false statements.

The SEC's announced priorities in connection with CETU signal a narrowed focus on investigating and bringing cybersecurity disclosure actions against public companies to those cases where the conduct rises to a higher level of misconduct. This potential shift would be consistent with a recent

dissent from now-Acting Chair Uyeda and Commissioner Peirce to cybersecurity settlements. This dissent would tend to indicate the new SEC's softening views on what it will consider to be material cybersecurity disclosures in the second Trump administration. In describing SolarWinds and its customers as "victims" of the cyberattacks between 2019 and 2022, Commissioners Peirce and Uyeda pointed to the Government Accountability Office, which characterized these cyberattacks as "one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and the private sector."[5] The Commissioners criticized the SEC's decision to immediately respond to this "attack against America" by "charging four customers of its Orion software, with violations of the federal securities laws." The dissenting statement further concluded that the settlements were demonstrative of the SEC "playing Monday morning quarterback" by second-guessing the companies' post-incident disclosures without focusing on whether the disclosures provided material information. The penalties totaled nearly $7 million, despite mitigating factors, such as cooperation and remediation efforts from the companies.

The Impact of SolarWinds

Another dynamic that may support a less aggressive approach to cybersecurity is the SEC's setback in the *SolarWinds* case. In July 2024, a federal court in New York dismissed most of the SEC's claims in its litigation against SolarWinds, while permitting the SEC to proceed with its securities fraud claims premised on a Security Statement that was posted on SolarWinds' website and authored by its CISO. For the remaining fraud claims, the court found that the SEC sufficiently pled that SolarWinds and its CISO misleadingly overstated the strength of the company's cybersecurity practices in the Security Statement, including:

- **Access Controls:** The SEC alleged that between 2017 and 2020, SolarWinds engaged in practices that resulted in the widespread grant of administrative rights to employees beyond what was necessary for employees' specific job functions despite representing that they maintained strong access controls.

- **Password Protections:** The SEC alleged that SolarWinds failed to enforce its password policies, as demonstrated by the use of "password" as a default password for a SolarWinds company product, and the use of "solarwinds123" as the password to one of the company's servers, despite representing that it required the use of complex passwords.

Discovery in the *SolarWinds* case is ongoing, with expert discovery set to have closed on February 14, 2025. The case is uniquely situated as the only time the SEC has tested fraud theories in an enforcement action related to cybersecurity. Even if the SEC prevails in this litigation, it is unclear how and to what extent a victory for the SEC will influence future investigations and cases in the Trump administration.

A Potential Rollback of the Cybersecurity Rules

The Cybersecurity Rules impose broad disclosure requirements on public companies aimed at enhancing and standardizing disclosures regarding cybersecurity risk management, strategy, governance, and material cybersecurity incidents. Both Acting Chair Mark Uyeda and Commissioner Peirce dissented from the adoption of the Cybersecurity Rules, largely criticizing the requirements as unnecessary, immaterial to investors, and burdensome for public companies.

There is uncertainty as to whether the SEC, when the new Chairman and new Commissioners are in place, will repeal or otherwise roll back the Cybersecurity Rules. On February 11, 2025, Acting Chair Uyeda announced that the SEC will not defend its climate disclosure rules that are currently being challenged in the Eighth Circuit. While Acting Chair Uyeda and Commissioner Peirce also dissented regarding the SEC's adoption of the climate disclosure rule, Acting Chair Uyeda's dissent regarding the climate disclosure rules was more critical of the authority of the SEC to regulate climate issues. For instance, Acting Chair Uyeda criticized these rules as exceeding the SEC's statutory authority or expertise to regulate "political and social issues," and questioned whether the agency "followed the proper procedures under the Administrative Procedure Act to adopt the Rule." It is unclear whether the Republican Commissioners will take a similar stance and ultimately consider repealing, or otherwise limit enforcing, the Cybersecurity Rules.

Takeaways

- **Cybersecurity continues to be an enforcement priority for the SEC, but the precise contours are unknown.** With the announcement regarding the CETU and its priorities, the SEC reinforced that cybersecurity disclosures have a place for now within its enforcement program.

- **For public companies, the SEC's announced focus on "fraudulent" cybersecurity disclosures potentially marks a likely shift away from SEC cybersecurity disclosure cases to date**. The SEC's cybersecurity disclosure actions have largely applied a consistent, but aggressive, approach in seeking negligence-based fraud charges and significant penalties despite mitigating factors such as cooperation and remediation. The cybersecurity enforcement landscape going forward may narrow with respect to the kinds of statements that the SEC will investigate, the types of charges the SEC will bring, and the penalties that the SEC may impose against public companies.

- **Companies should be cognizant of the pre-existing SEC enforcement landscape, which emphasizes the importance of disclosure and escalation procedures in the wake of a major cybersecurity incident.** These cases underscore that the SEC expects public companies to have well-defined and functioning disclosure practices and committees to ensure that important information is presented to the proper decision-makers, in order to make timely materiality determinations.

- **Companies should also be mindful of the broader disclosure and enforcement landscape.** Covered entities subject to the Cybersecurity Infrastructure and Security Agency (CISA)

disclosure rule will still be obligated to disclose cybersecurity events to CISA within three days. Further, companies who experience cybersecurity incidents involving compromised personal identifying data may have disclosure obligations based on state data breach laws, and they may be subject to private class action litigation and state attorney general enforcement actions. As a result, companies should continue to develop and implement strong procedures for managing and disclosing cybersecurity incidents regardless of how the SEC may enforce the Cybersecurity Rule.

Ultimately, public companies face considerable challenges in making appropriate disclosure decisions about their cybersecurity practices and, in the event of a cybersecurity incident, at the time of discovery of the incident and during the pendency of the investigation and remediation. Companies should ensure that they are prepared—from an incident response and disclosure policy perspective—before a major cybersecurity incident, and they should consult with counsel if faced with difficult disclosure decisions in the event of an incident.

Footnotes

[1] *See* Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors (Mar. 9, 2023), https://www.sec.gov/news/press-release/2023-48.

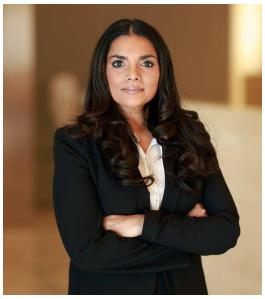
[2] *Id.*

[3] *Id.*

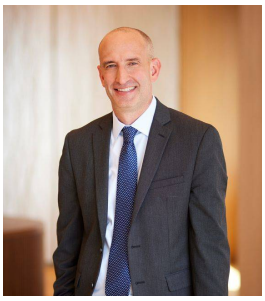
[4] Gurbir S. Grewal, Director, U.S. Sec. & Exch. Comm'n Div. of Enf't, Remarks at Financial Times Cyber Resilience Summit (June 22, 2023), https://www.sec.gov/news/speech/grewal-financial-times-cyber-resilience-summit-06222023.

[5] *See* Press Release, U.S. Sec. & Exch. Comm'n, Statement Regarding Administrative Proceedings Against SolarWinds Customers (Oct. 22, 2024), https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-solarwinds-102224.

Related Attorneys



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605



Charles D. Riely
Partner
criely@jenner.com
+1 212 891 1686

H. Kurt von Moltke
Partner
kvonmoltke@jenner.com
+1 312 840 7499

Kathryn Chang
Associate
kchang@jenner.com
+1 212 407 1767

Philip B. Sailer
Associate
psailer@jenner.com
+1 312 840 7267

Related Capabilities

Business Litigation

Corporate

Data Privacy and Cybersecurity

Investigations, Compliance, and Defense

© 2026 Jenner & Block LLP. Attorney Advertising. Jenner & Block LLP is an Illinois Limited Liability Partnership including professional corporations. This publication, presentation, or event is not intended to provide legal advice but to provide information on legal matters and/or firm news of interest to our clients and colleagues. Readers or attendees should seek specific legal advice before taking any action with respect to matters mentioned in this publication or at this event. The attorney responsible for this communication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome. Jenner & Block London LLP, an affiliate of Jenner & Block LLP, is a limited liability partnership established under the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with SRA number 615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed →