GT GreenbergTraurig

Alert | Data Privacy & Cybersecurity/ Securities Litigation

October 2024

SEC Files Actions Against 4 Public Companies for Negligent Cybersecurity Disclosures

Go-To Guide:

- The Securities and Exchange Commission settled actions against four technology companies for "negligently minimizing" the impact of the 2020 SolarWinds Orion software breach in public filings.
- The SEC found that the companies had described their cybersecurity incident risks as hypothetical, despite knowing that the breaches had occurred, or that they minimized the scope of the attacks.
- The SEC cited one company for inadequate cybersecurity disclosure controls and procedures.
- The four actions double the SEC's public company cybersecurity disclosure cases and underscore its continued prioritization of cyber breach public disclosures.

On Oct. 22, 2024, the SEC announced settled administrative actions against four current or formerly public technology companies, finding that the companies all made materially misleading disclosures to investors in their periodic filings concerning the impact of the 2020 SolarWinds breach on their businesses. The SEC's orders allege that the companies learned in 2020 or 2021 that the threat actor responsible for perpetrating the SolarWinds breach had also accessed their systems, but – according to the SEC's press release announcing the settlements – misled investors by "negligently minimiz[ing]" their respective incidents in their public disclosures in various ways. The SEC found that two of the companies had described their risks from cybersecurity incidents as hypothetical or generic, despite knowing that

actual incidents had occurred, and such risks had materialized. The SEC found that the other two companies had minimized the scope of the attacks on their respective networks by failing to disclose the full extent of the accessed or exfiltrated data.

The SEC found that one company had deficient disclosure controls and procedures, which purportedly contributed to the misleading disclosures.

The four companies paid approximately $7 million in civil monetary penalties.

Background

The SEC filed its first cybersecurity disclosure action against a public company in 2018 for allegedly negligently failing to disclose in its public filings a massive breach for more than two years, charging violations of Section 17(a) of the Securities Act, as well as failing to maintain adequate disclosure controls and procedures related to cybersecurity pursuant to Securities Exchange Act Rule 13a-15. In 2021, the SEC filed cybersecurity disclosure actions against two public companies alleging negligent misleading statements or omissions in their public disclosures and/or Rule 13a-15 violations.

In October 2023, the SEC filed its first cybersecurity disclosure enforcement action alleging scienter-based fraud – instead of negligence – against SolarWinds and its chief information security officer, Tim Brown, in connection with a cyberattack perpetrated against SolarWinds in 2020 by Russian state actors. The case was the first time the SEC had charged an individual executive in connection with a public company cybersecurity disclosure action. In July 2024, the U.S. District Court for the Southern District of New York dismissed the SEC's claims against SolarWinds and Brown regarding the adequacy of SolarWinds' cybersecurity disclosures concerning the 2020 breach, finding the SEC had impermissibly relied on "hindsight and speculation" to find those disclosures fraudulent. In August 2024, the parties disclosed to the court that they were discussing settling the remaining fraud claims.

Cybersecurity disclosures have also been the subject of recent SEC rulemaking. In July 2023, the SEC adopted a rule, effective December 2023, requiring public companies to disclose material cybersecurity incidents under Item 1.05 of Form 8-K within four days of determining an incident was material, or, for foreign private issuers, on Form 6-K "promptly" after the incident is disclosed or otherwise publicized. The four-day deadline to disclose on Form 8-K may be extended if the U.S. attorney general determines that disclosure would pose a substantial risk to national security or public safety, but such an extension may be rare. The rule also requires companies to provide cybersecurity risk management, strategy, and governance disclosures set forth in Item 106 of Regulation S-K in its annual filings on Form 10-K, and, for foreign private issuers, comparable disclosures on Form 20-F.

Takeaways

- The four actions underscore the SEC's continued prioritization of cyber breach disclosures by public companies and related disclosure controls and procedures.
- They also represent a return to negligence-based charges related to public companies' cyber disclosures on, e.g., Forms 10-K and 8-K after the July 2024 SolarWinds decision dismissing similar fraud charges.
- Several of the orders favorably note the companies' cooperation with the SEC investigation, consistently mentioning that the companies provided the staff with "detailed explanations, analysis, and summaries" of factual issues, conducted internal investigations and shared the findings with the SEC staff "on [their] own initiative," and took steps "to enhance [their] cybersecurity controls."

- None of the cases cite the new cybersecurity disclosures rule the SEC adopted in July 2023 because the conduct at issue occurred prior to its effective date. The SEC may continue to scrutinize public companies' cyber disclosures in detail, including their decisions concerning the quantitative and qualitative materiality of cyber incidents, as well as decisions whether to file disclosures on the new Item 1.05 of Form 8-K or, for foreign private issuers, on Form 6-K, and the timing of such disclosures relative to the rule.
- Public companies should review their disclosure controls and procedures to ensure they address cybersecurity incident reporting and disclosure, and review their cybersecurity risk management, strategy, and governance disclosures in their periodic filings carefully to ensure fulsome descriptions, where appropriate, of known material incidents or risks.

Authors

This GT Alert was prepared by:

- Tracy S. Combs | +1 415.655.1300 | Tracy.Combs@gtlaw.com
- Barbara A. Jones | +1 310.586.7773 | Barbara.Jones@gtlaw.com
- Steven M. Malina | +1 312.476.5133 | Steven.Malina@gtlaw.com
- Marc M. Rossell | +1 212.801.6416 | rossellm@gtlaw.com
- Jena M. Valdetero | +1 312.456.1025 | Jena.Valdetero@gtlaw.com
- Daniel J. Wadley | +1 801.478.6910 | wadleyd@gtlaw.com
- David A. Zetoony | +1 303.685.7425 | David.Zetoony@gtlaw.com