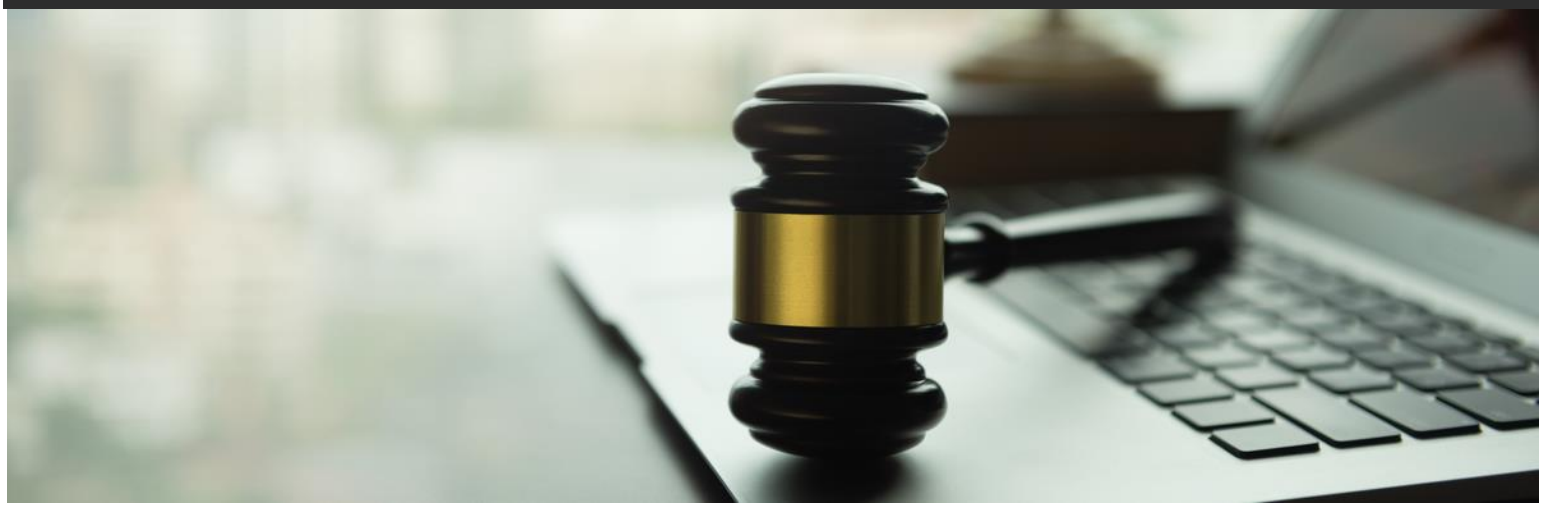
GT GreenbergTraurig

Alert | Data Privacy & Cybersecurity



July 2024

SEC v. SolarWinds Update: U.S. Federal District Court Dismisses Most of the SEC's Case, but Some Fraud Claims and CISO Liability Remain

Go-To Guide:

- A U.S. district court dismissed all the SEC's securities fraud and false filings claims against SolarWinds and its Chief Information Security Officer (CISO) Timothy Brown regarding the adequacy of cyberattack disclosures, finding that the SEC had impermissibly relied on "hindsight and speculation" to find those disclosures fraudulent.
- The court also dismissed the SEC's claims that SolarWinds' cybersecurity deficiencies amounted to deficient internal accounting controls, finding that the SEC had stretched the definition of "accounting" past its limit.
- But the decision wasn't a wholesale win for SolarWinds or Brown. The court upheld the SEC's scienter-based fraud claims against both parties related to the security statement posted on SolarWinds' website prior to the attack, finding the statement actionable under the securities laws, and that Brown could also be held potentially liable under Section 10(b) of the Exchange Act and Section 17(a) of the Securities Act for its false and misleading content.
- Public companies' statements related to their cybersecurity practices are still a major risk area for the companies, their CISOs, and potentially other executives as well.

In December 2020, a SolarWinds customer reported a vulnerability in its flagship Orion software platform resulting from a threat actor inserting a malicious code. The code infiltrated thousands of companies' networks and became known as the "SUNBURST" cyberattack.

The SEC's case is notable because it is the first in which the SEC (1) brought an action for scienter-based fraud—not simple negligence under Section 17, as in prior cases—related to a company's cybersecurity disclosures; (2) charged an individual executive—here, SolarWinds' CISO—in a cybersecurity disclosure case; and (3) brought charges against a company for failure to devise and maintain adequate internal accounting controls regarding cybersecurity under Section 13(b)(2)(b) of the Exchange Act.

In its amended complaint, the SEC asserted fraud claims against SolarWinds and Brown based on pre- and post-SUNBURST statements to investors, alleging that SolarWinds misled the public by: (1) publishing a security statement that reflected robust cybersecurity practices, knowing that it was vulnerable to cybersecurity risks; (2) minimizing the scope and severity of the attack in its SEC filings; and (3) making statements in blog posts, podcasts, and press releases that misstated the strength of the company's cybersecurity.

The July 18, 2024, Decision

Fraud Claims Based on the Security Statement Upheld

The U.S. District Court for the Southern District of New York upheld the SEC's fraud claims under Section 10(b) of the Exchange Act and Section 17(a) of the Securities Act against SolarWinds and Brown (as well as aiding and abetting liability for Brown) as to SolarWinds' online security statement, posted on its website before the SUNBURST attack.

The decision found that "false statements on public websites" can sustain liability under the securities laws if accessible to investors,[1] finding that the SEC had adequately pled that SolarWinds' "overall portrait" of its cybersecurity was "misleading if not outright false" given that Brown and the company knew that SolarWinds' access control and password protection systems had received poor marks under its NIST Cybersecurity Framework assessments and internal SOX audits, and that Brown was aware of specific security vulnerabilities.

In light of that knowledge, the decision stated that Brown's conduct "in allowing the Statement to issue publicly, and to remain in place for years . . . is plausibly pled as highly unreasonable or extreme misconduct" (internal quotes and citation omitted).

Fraud Claims Based on Brown's Statements in Press Releases, Blog Posts, and Podcasts Dismissed

The court dismissed the SEC's fraud claims based on statements Brown made in other publicly available forums, regarding SolarWinds' cybersecurity practices as "non-actionable corporate puffery" that were "too general" for a reasonable investor to rely upon.

Fraud Claims Based on SolarWinds' SEC Filings Dismissed

The court dismissed the SEC's fraud claims (under both its misrepresentation and scheme liability theories) and false filings claims under Section 13(a) of the Exchange Act as to all of SolarWinds' SEC

[1] Notably, the court sustained both the SEC's misrepresentation and scheme liability theories as to both defendants under the antifraud provisions, citing the Second Circuit's recent decision in *SEC v. Rio Tinto* (2022) in finding that dissemination of the security statement to investors was the "something beyond" misstatements and omissions required to sustain scheme liability.

filings cited in the amended complaint, including its cybersecurity risk disclosures and its Form 8-Ks disclosing the SUNBURST attack.

First, the court addressed SolarWinds' cybersecurity risk disclosures in its 2018 IPO registration statement (Form S-1) and incorporated by reference in subsequent annual and quarterly reports (Forms 10-K and 10-Q) and offering documents (Form S-8), which the SEC argued were misleading because they did not acknowledge the security vulnerabilities SolarWinds knew it faced or prior known cyberattacks, and that SolarWinds failed to amend those risk disclosures as its knowledge concerning pre-SUNBURST incidents developed.

The court dismissed the SEC's claims under a misrepresentation theory, finding that a reasonable investor could not have been misled by the risk disclosures because they sufficiently detailed the corporation's vulnerabilities to security breaches, laid out the potential consequences of a breach on its financial health, and disclosed that SolarWinds might be unable to detect or prevent such attacks. Notably:

- The court found "the SEC's liability theory" on SolarWinds' failure to update the risk disclosures to account for specific pre-SUNBURST incidents was "conceptually sound" under the applicable case law, but in this specific instance, the SEC had inadequately pled that the incidents sufficiently undermined the company's risk disclosures because they were broad enough to cover the specific risks posed by those more minor incidents.
- While the SEC's amended complaint faulted SolarWinds' risk disclosures for failing to disclose the pre-SUNBURST attacks as likely precursors to the SUNBURST attack itself, the court found that conclusion was based on hindsight, and that the risk disclosures should be evaluated based on "the information the company had in real time and the conclusions it reasonably drew from that information."
- The court found that the amended complaint did not adequately plead that Brown deliberately concealed SolarWinds' cybersecurity deficiencies from top-level executives responsible for creating the risk disclosures who knew, or should have known, that the pre-SUNBURST incidents rendered the disclosures misleading.

Second, the court addressed the SEC's claim that SolarWinds' December 2020 Form 8-Ks disclosing the SUNBURST attack were materially misleading because they did not disclose the earlier, more minor cybersecurity incidents, again noting that "perspective and context" were critical to evaluating the 8-Ks, which were released "at an early stage of [SolarWinds'] investigation, and when its understanding of that attack was evolving."

Internal Controls Claims Dismissed

The court found equally unconvincing the SEC's claims against SolarWinds under Section 13(b)(2)(b) of the Exchange Act alleging the corporation failed to establish and maintain appropriate internal accounting controls because its poor cybersecurity controls could have caused unauthorized access to SolarWinds' accounting systems. In rejecting this argument, the court described it as "ill-pled" and "not tenable," because Section 13(b)(2)(b) of the Exchange Act was, by its own language, limited to a company's internal financial accounting controls and was not intended to apply to cybersecurity controls.

Finally, the court rejected the SEC's claim against SolarWinds under Exchange Act Rule 13a-15(a), which requires companies to maintain adequate disclosure controls and procedures designed to ensure that information required to be reported in periodic filings is timely and adequately disclosed. The court found

that the SEC did not plead any "deficiency in the construction" of SolarWinds' disclosure controls and procedures, nor that the system generated numerous errors.

SolarWinds is required file an answer to the SEC's amended complaint by Aug. 1, 2024.

Takeaways

- The decision underscores that a company's disclosures of a cyber incident could only be based on what the company and its executives knew about the incident at the time the disclosures were made, hindering the SEC's ability to second-guess the adequacy of those disclosures years later.
- The ruling may signal the end of the SEC's ability to bring Section 13(b)(2)(b) charges relative to cybersecurity unless it can point to actual financial accounting deficiencies that affected the company's ability to assess the incident's effect on its financial statements.
- Although most of the claims against Brown were dismissed, CISOs should not take too much comfort in the ruling, as they may remain personally liable, at least at the pleading stage, for making false statements to investors regarding their company's cybersecurity practices. CISOs should take care when balancing candid internal discussions about cybersecurity vulnerabilities with what is disclosed to the public.

Authors

This GT Alert was prepared by:

- Tracy S. Combs | +1 415.655.1300 | Tracy.Combs@gtlaw.com
- Steven M. Malina | +1 312.476.5133 | Steven.Malina@gtlaw.com
- Jena M. Valdetero | +1 312.456.1025 | Jena.Valdetero@gtlaw.com
- Nair Marie Banks III | +1 312.476.5002 | Nair.Banks@gtlaw.com

not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2024 Greenberg Traurig, LLP. All rights reserved.