Davis Polk

Mixed result for SEC in cyber disclosure case against SolarWinds and its CISO

July 24, 2024 | Client Update | 6-minute read

A court rendered a mixed result in the SEC's SolarWinds litigation. The court declined to dismiss the SEC's claims that a website "Security Statement" overstated the strength of SolarWinds' cybersecurity measures. However, the court dismissed claims based on SolarWinds' SEC filings after discovery of a cybersecurity incident and also dismissed claims that SolarWinds lacked adequate accounting and disclosure controls, a setback for the SEC in its expansive reading of the controls requirements.

Background

In October 2023, the SEC brought a much-publicized enforcement action against SolarWinds Corporation and Timothy Brown, the VP of its information security group, alleging that the company made misleading cybersecurity disclosures and had internal control failures. SolarWinds, a Texas-based publicly-traded company, sells software that companies and governments use to manage their computer systems. SolarWinds was the victim of a nearly two-year cyberattack, known as SUNBURST, which the company first disclosed in December 2020, resulting in a substantial drop in its stock price.

The SEC alleged that SolarWinds misled investors in several ways. First, the SEC alleged that a "Security Statement" posted on the company's website, which was directed at the company's customers, made false statements about the strength of the company's security practices. These included statements that the company met industry standards, used a secure developmental lifecycle, implemented network monitoring, had strong password protections, and maintained good access controls. The SEC also alleged that SolarWinds made similar misleading disclosures in SEC filings and public statements, such as press releases, blog posts, and podcasts. Finally, the SEC alleged that the company made incomplete disclosures about the SUNBURST attack in its SEC filings after the attack.

The SEC's action against Brown centered on allegations that he was aware of the company's cybersecurity risks and vulnerabilities, was responsible for the website Security Statement, and was involved in the other filings and statements. Among other things, the SEC highlighted internal communications involving Brown in which he raised concerns about the company's ability to protect critical assets from cyberattacks.

The SEC further alleged that SolarWinds lacked reasonable internal accounting controls to prevent unauthorized access to company assets, in this case its information technology, source code and software products. The SEC equated the company's cybersecurity measures, which were intended to prevent unauthorized access to its "most critical assets," with the internal accounting controls issuers are required to maintain pursuant to Section 13(b)(2)(B) of the Securities Exchange Act of 1934. The SEC further alleged SolarWinds had deficient disclosure controls and procedures in violation of Exchange Act Rule 13a-15 because it alleged that information regarding material cybersecurity risks, incidents, and vulnerabilities was not timely escalated to senior management with disclosure-related responsibilities.

The court's decision

On July 18, 2024, Judge Paul Engelmayer of the U.S. District Court for the Southern District of New York granted, in substantial part, SolarWinds and Brown's motions to dismiss the SEC's disclosure and controls-related claims. However, the court permitted a core aspect of the SEC's case tied to the company's website Security Statement to proceed to discovery.

The court ruled that the SEC had sufficiently pled that statements in the Security Statement about SolarWinds' access controls and password practices were materially misleading by a "wide margin." The court found the alleged misstatements were material because cybersecurity was a "key attribute" for the company's software products. The court rejected the defendants' arguments that the Security Statement should not be the foundation for a claim because it was directed to customers, not investors. The court said that the website information was part of the "total mix of information" available to investors. The court also found that the SEC had sufficiently pled that Brown acted with fraudulent intent because he allegedly was aware of internal information that was inconsistent with the Security Statement.

The court took a dim view of the remaining SEC allegations. The court dismissed the SEC's claims about press releases, blog posts, and podcasts because they were non-specific "corporate puffery" on which a reasonable investor would not rely. With respect to its SEC filings, the court ruled that SolarWinds did not have an obligation to update its cybersecurity risk disclosures and related statements. The court noted that the company had sufficiently warned investors about the serious threat of cyberattacks and cyber intrusions.

The court likewise rejected the SEC's allegations that the company's December 2020 disclosures on Form 8-K regarding the SUNBURST cyberattack were misleading. The court noted that the Form 8-K disclosures "bluntly reported bad news" for the company just days after the discovery of the cyberattack and disclosed the information known to the company "with appropriate gravity and detail."

Finally, the court rejected the SEC's claims that the Exchange Act requirements for internal accounting controls also include requirements for cybersecurity controls. As the court explained, this requirement "does not govern every internal system a public company" uses to safeguard corporate assets, only those qualifying as internal accounting controls concerning *financial* transactions and events. The court found support for this interpretation in the Foreign Corrupt Practices Act of 1977, which enacted the accounting controls provision as part of congressional efforts to promote more accurate financial reporting in the wake of foreign bribery scandals.

The court similarly rejected the SEC's disclosure controls claim under Rule 13a-15 of the Exchange Act, noting that the company did, as pled by the SEC, in fact have a system of controls to ensure the disclosure of potentially material cybersecurity risks and incidents. Although SolarWinds had erroneously classified two cyber incidents under its incident response plan, those errors alone did not indicate that the company's disclosure controls were inadequate. As the court explained, "errors happen without systemic deficiencies."

Takeaways

We see a few immediate implications of the court's ruling.

- **Statements outside of SEC filings**. The ruling is an important reminder that statements outside of SEC filings, about cybersecurity or other topics deemed material to investors, can be the basis for an SEC enforcement investigation or civil litigation. This is true even for statements that are not directed at investors but that are publicly disseminated in some fashion (the Security Statement on the company's website was directed at customers). We expect the SEC to continue to scrutinize statements about cybersecurity, ESG, and other topics beyond the traditional focus on financial performance regardless of the intended audience.
- **Second-guessing cybersecurity event disclosures**. The court's dismissal of the SEC claims about SolarWinds' post-event disclosures is a promising development. Cybersecurity events often are fast-moving, and it can be challenging for issuers to decide what and when to disclose. This case was filed before the SEC's new cybersecurity disclosure rules were in effect (see our client update summarizing those rules), but the court's characterization of the SEC's claims as "impermissibly rely[ing] on hindsight and speculation" should be a helpful precedent in countering attempts by the government and private plaintiffs to second-guess good-faith cybersecurity disclosure decisions.
- **Setback for the SEC on accounting controls**. The SEC suffered a significant loss with the court's rejection of its expansive interpretation of the accounting controls provision. In recent years, the SEC has brought a series of settled actions alleging internal accounting controls violations in circumstances unrelated to the financial reporting process. For example, the SEC has alleged accounting controls violations in connection with stock buyback arrangements (see our prior client updates here and here) and just a few weeks ago, announced a settlement alleging that a company's cybersecurity controls violated the internal accounting controls provisions. That case drew a vigorous dissent on similar grounds as the court's decision in SolarWinds. With most of the SEC's efforts to expand the accounting

controls provision taking place in settled proceedings, this rejection by a federal judge provides support to companies in pushing back against expansive SEC controls theories.

– **Disclosure controls and procedures**. In dismissing the SEC's disclosure controls claim, the court made clear that the Exchange Act does not require perfection. The fact that a few errors may occur does not render a company's controls inadequate, and the SEC must allege "systemic deficiencies." The court's ruling provides companies facing SEC scrutiny with additional grounds to push back on expansive disclosure controls theories.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Maurice Blanco
+55 11 4871 8402
+1 212 450 4086
maurice.blanco@davispolk.com

Micah G. Block
+1 650 752 2023
micah.block@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

Marcel Fausten
+1 212 450 4389
marcel.fausten@davispolk.com

Michael Kaplan
+1 212 450 4111
michael.kaplan@davispolk.com

John B. Meade
+1 212 450 4077
john.meade@davispolk.com

Paul J. Nathanson
+1 202 962 7055
+1 212 450 3133
paul.nathanson@davispolk.com

Fuad Rana
+1 202 962 7053
fuad.rana@davispolk.com