On the WLF Legal Pulse

Timely commentary from WLF's blog July 24, 2024

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

SDNY's Rejection of SEC's Novel Internal Control Claim in SolarWinds Offers Guidance on Cybersecurity Disclosure

by Gregory A. Brower, Emily R. Garnett, and Jack L. Hobaugh Jr.

On July 18, 2024, a U.S. Southern District of New York judge issued a much-anticipated decision on a motion to dismiss filed by the SolarWinds Corp. ("SolarWinds") and its former vice president for information security, Timothy G. Brown ("Brown"). The motion asked Judge Paul Engelmayer to dismiss the U.S. Securities and Exchange Commission's ("SEC") complaint for misrepresentations arising from a historic cybersecurity breach. Judge Engelmayer issued a 107-page opinion, ultimately ruling that most of the SEC's claims survive the defendants' motion, but most notably dismissing the SEC's novel theory that the cyber breach violated the company's internal accounting controls.

As we've previously written, SolarWinds sells high-end security software to the government and private entities, including its well-known "Orion" software program. The SEC contended that, contrary to SolarWinds' public representations and marketing materials, its cyber products were not secure and were at significant risk of cyberattacks. In particular, the SEC alleged SolarWinds mislead the public about a large-scale cyberattack—known as "SUNBURST," which purportedly was conducted by state-sponsored hackers in Russia—and brought charges under the Securities Act of 1933, the Securities Exchange Act of 1934 and related rules.

The SEC focused its claims on various sources of SolarWinds' public statements, including its Security Statement and the cybersecurity "Risk Disclosure" in the company's SEC filings, including its Form S-1 Registration Statement and 8-Ks filed immediately after the cyberattack, as well as press releases, podcasts and blog posts. The SEC further alleged SolarWinds violated Section 13(b)(2)(B) of the Securities Exchange Act because of its ineffective internal controls and procedures. Although the order is not subject to automatic appeal, we expect the SEC may move for interlocutory appeal so that it can take another swing at its accounting internal control claim (given the legal holding, the SEC is unlikely to simply amend the complaint). We also expect this decision will serve as important guidance for cybersecurity professionals, accounting teams and internal control and audit teams as well as in-house and outside counsel as they navigate the expanding obligations companies face as it relates to cybersecurity disclosures.

Gregory A. Brower, **Emily R. Garnett**, and **Jack L. Hobaugh Jr.** are Shareholders with Brownstein Hyatt Farber Schreck, LLP. Mr. Brower serves on WLF's Legal Policy Advisory Board and is a Featured Expert Contributor to the *WLF Legal Pulse* blog.

The Court Dismissed the SEC's Novel Accounting Control Claim Arising from the Cyberattack

On March 22, 2024, the defendants moved to dismiss each claim of the SEC's amended complaint and each of its underlying claims. After the parties filed their respective briefs, the court heard argument on May 15, 2024. From then, industry professionals patiently awaited the court's ruling.

As highlighted above, perhaps the most notable portion of Judge Engelmayer's order was his decision to grant the defendants' motion to dismiss the SEC's accounting control claim. The SEC previously acknowledged that this case was the "first in which it has brought an accounting control claim based on an issuer's cybersecurity failings," premised on the SEC's newly adopted cybersecurity rules from July 2023.

Despite numerous and broad-based allegations of systemic cybersecurity failures, the court found this was not enough to establish internal accounting control failures. Such allegations include assertions that SolarWinds knew and had presented on its "very vulnerable state for our critical [security] assets," as early as August 2017—warnings which came a year before the company's public offering and were revisited repeatedly until the cyberattacks that began in January 2019 and continued through December 2020. The SEC pointed to internal assessments conducted by the company under the "NIST Framework," wherein the Company scored itself on a scale of "0" to "5" in five areas—and whereby the company gave itself a "0" and "1" in several areas for multiple years. The SEC also alleged that SolarWinds' practices around password requirements, access controls, authentication and identity management were well-known areas of vulnerability that the Company failed to address. The court found that the SEC adequately alleged at least the Security Statement misrepresentations related to access controls and password protection policies.

Defendants argued that the statute defining a "system of internal accounting controls" is not so broad as to cover a company's cybersecurity controls such as its password and VPN protocols. The court agreed, interpreting the term to mean "a company's *financial accounting*," and in turn, defining the term "accounting" to refer to "transactions," "preparation of financial statements," "generally accepted accounting principles," and "books and records." The court noted that nowhere in the legislative history did Congress intend to include cybersecurity in the definition of "a system of internal accounting controls," stating, "That is no surprise. The statute was enacted in 1977—long before cybersecurity became a relevant concept in business or society." And while the court recognized that cybersecurity assets are important to an enterprise and its internal controls, this does not outweigh Congress's attempt to limit oversight to "internal accounting controls" only, reasoning "Congress does not 'hide elephants in mouseholes.'" To add some perspective, in the mid-1970s, programmers were still submitting programs and the associated data to a computer operator on punch cards. The internet did not become publicly available until 1993. Indeed, cybersecurity was not an issue in 1977.

We would anticipate the SEC may move for interlocutory appeal so that it can further litigate this issue. But now with the Supreme Court's recent decision overturning *Chevron* deference, the SEC faces challenging terrain ahead to convince the Second Circuit that its interpretation of "internal accounting controls" includes cybersecurity assets.

The Court Provides Helpful Guidance on a Company's Risk Statement and 8-K

In addition to the court's discussion on the internal control claim, the court also went into some length about SolarWinds' cyberattack risk disclosure as to whether—as the SEC alleged—it was "unacceptably boilerplate and generic." Relevant to practitioners, the court rejected the SEC's

© 2024 Washington Legal Foundation

position, finding that the disclosures adequately set out in some detail the risks the company faced, quoting at length the SolarWinds' disclosure and finding, in totality, it was "sufficient to alert the investing public of the types and nature of the cybersecurity risks that SolarWinds faced and gave consequences these [risks] could represent for the company's financial health and future." The court rejected the SEC's argument that the disclosures should have been more specific, finding that the case law and anti-fraud laws "do not require cautions to be articulated with maximum specificality," warning that a more specific and narrow statement could actually be more likely to mislead an investor about the risk of an attack.

Nor did the court find the SEC had adequately alleged SolarWinds or Brown systematically conspired to mislead the public about the SUNBURST attacks in the company's 8-K filings. The court found that, read fairly and in totality, the Form 8-K disclosure—filed just two days after the attack became known—adequately informed investors of the attack, whereby the court parsed the expression "successful exploitation" to determine whether a reasonable investor could easily read that term to connote more consequential or damaging events. Like the company's Risk Disclosure, the Company's 8-K filing serves as an important and useful standard for issuers to potentially model if they suffer a cyberattack.

For cybersecurity professionals and their disclosure counsel, this portion of the opinion provides several helpful tips on how to constructively advise the public about a potential or known cyberattack, even as the company's investigation is ongoing.

© 2024 Washington Legal Foundation