July 23, 2024

SDNY Court Deals Blow to SEC Cyber Enforcement, Dismisses Most Charges Against SolarWinds and Its CISO

On July 18, 2024, Judge Paul A. Engelmayer of the U.S. District Court for the Southern District of New York ("SDNY") granted in large part a motion by SolarWinds Corporation ("SolarWinds") and Timothy Brown, SolarWinds' Chief Information Security Office ("CISO"), to dismiss a civil suit filed against them by the Securities and Exchange Commission ("SEC").[1] The motion to dismiss was supported by four groups that submitted amicus briefs, including a brief submitted by Paul, Weiss on behalf of former government officials.

When filed, the case marked a number of firsts for the SEC: the first time it had brought intentional fraud charges in a cybersecurity disclosure case, the first time it had brought an accounting control claim based on an issuer's alleged cybersecurity failings, and the first time it had brought a cybersecurity enforcement claim against an individual. The SEC based its claims on alleged material misrepresentations and omissions by SolarWinds and Brown, both before and after the company disclosed a large-scale cyberattack, known as SUNBURST, in December 2020. Specifically, the SEC alleged that SolarWinds and Brown had misleadingly touted the company's cybersecurity practices before the incident, including in a security statement published on the company's website, in a cybersecurity risk disclosure made in SolarWinds' SEC filings, and in press releases, podcasts and blog posts. The SEC also alleged that the company's Form 8-K disclosures following the SUNBURST incident minimized the scope and severity of the attack. Additional claims were premised on SolarWinds' purported failure to maintain effective internal accounting and disclosure controls and procedures for identifying and disclosing cybersecurity risks.[2]

The only set of claims sustained by the court were the claims against SolarWinds and Brown for securities fraud based on the security statement on the company's website, which claims the court held were viably pled as materially false and misleading in numerous respects. The court dismissed the claims of securities fraud and of false filings based on other statements and filings, as well as all of the claims based on SolarWinds' post-SUNBURST disclosures. The court also dismissed the SEC's claims relating to SolarWinds' internal accounting and disclosure controls and procedures.

Key Takeaways

- **Specific false or misleading statements on a company's public website about the state of a company's cybersecurity, even if the statements are directed to customers rather than investors, can be the basis for securities fraud liability**: The court declined to dismiss the SEC's claims related to a security statement published on a SolarWinds website, explaining that the

[1] The SEC brought claims under Section 10(b) of the Securities Exchange Act of 1934, 15 U.S.C. § 78j(b), and its implementing rule, Rule 10b-5(b); Section 13(a) of the Exchange Act, 15 U.S.C. § 78m(a), and its implementing rules, Rules 12b-20, 13a-1, 13a-11 and 13a-13; and Section 17(a) of the Securities Act of 1933, 15 U.S.C. § 77q(a).

[2] The SEC's internal accounting control claim was brought under Section 13(b)(2)(B) of the Exchange Act, 15 U.S.C. § 78m(b)(2)(B). The SEC's disclosure controls and procedures claim was brought under Exchange Act Rule 13a-15(a).

statement was accessible to investors and therefore part of the "total mix of information" that SolarWinds furnished to the investing public.[3] According to the amended complaint, Brown approved and disseminated the security statement despite being privy to internal information that contradicted the statement's representations about the company's access controls and password practices. The court determined that the alleged misrepresentations, as pled, were materially misleading and that the allegations sufficiently pleaded Brown's knowledge of, or at least recklessness as to, the misstatements on SolarWinds' website. Additionally, the court concluded that Brown's scienter was properly imputed to SolarWinds. Although it remains to be seen whether the evidence will support the allegations, the fact that these claims based on a public security statement were the only claims to survive the motion to dismiss, serves as an important reminder that all public statements about a company's cybersecurity practices, not only those in SEC filings, can have legal consequences and should therefore be carefully reviewed for accuracy.

- **"Internal accounting controls" do not extend to cybersecurity controls**: The court held that Section 13(b)(2)(B) of the Exchange Act, which requires an issuer to devise and maintain "internal accounting controls," is limited to controls related to accounting and does not extend to cybersecurity controls, such as password and VPN protocols. As the court explained, the Exchange Act "does not govern *every internal system* a public company uses to guard against unauthorized access to its assets, but only those qualifying as 'internal accounting' controls."[4] "Cybersecurity controls," stated the court, "are undeniably vitally important, and their failures can have systemically damaging consequences. But these controls cannot fairly be said to be in place to 'prevent and detect errors and irregularities that arise in the accounting systems of the company.'"[5]

  If the decision stands, it could limit the SEC's ability to pursue Exchange Act claims related to internal controls that do not relate specifically to the company's financial statements. And the SEC could therefore lose an important tool for public company cybersecurity enforcement. Just last month, the SEC announced that R.R. Donnelley & Sons Co. had agreed to pay $2.1 million to settle charges that the company failed to maintain "cybersecurity-related internal accounting controls" and to design effective disclosure controls to report relevant cybersecurity information to management.[6] The SolarWinds decision may make it more difficult for the SEC to settle internal accounting controls claims based on allegedly deficient cybersecurity controls.

- **Cybersecurity risk disclosures and disclosure controls can provide important defenses to securities fraud claims**: The court reiterated that risk disclosures do not need to be stated with maximum specificity and detail under the securities laws, and found that SolarWinds had adequately identified in its disclosures the nature and types of cyber risks that it faced and associated consequences. Moreover, the court seemed to attach significance to SolarWinds' ability to promptly assess whether disclosures of material information to the investing public were needed, and to file a Form 8-K disclosing the cyberattack within a matter of days. In the court's view, "[p]erspective and context are critical" when evaluating whether SolarWinds' Form 8-K was sufficiently pled as materially misleading; considering the "short turn-around" in which SolarWinds was able to file its Form 8-K disclosing the SUNBURST attack, it contained "appropriate gravity and detail."[7]

---

3 *See SEC* v. *SolarWinds Corp.*, No. 23 Civ. 9518 (PAE), Opinion at 51 (July 18, 2024), hereinafter, "Opinion."

4 *Id.* at 100 (emphasis in original).

5 *Id.* at 98–99 (quoting *SEC* v. *World-Wide Coin Invs., Ltd.*, 567 F. Supp. 724, 750 (N.D. Ga. 1983)).

6 *SEC Charges R.R. Donnelly & Sons Co. with Cybersecurity-Related Controls Violations*, Sec. & Exch. Comm'n, Press Release 2024-75 (June 18, 2024), https://www.sec.gov/newsroom/press-releases/2024-75.

7 Opinion at 86.

Background on the SEC's Suit and the Court's Decision

According to the SEC's lawsuit, in January 2019, threat actors secured access to SolarWinds' corporate VPN and proceeded to exploit that connection to access SolarWinds' network.[8] The threat actors subsequently inserted malicious code into SolarWinds' software.[9] The threat actors leveraged this malicious code to conduct a series of cyberattacks, later referred to as SUNBURST, which impacted the operations of many of its customers, including federal and state government agencies.[10] After learning of the SUNBURST attack, Brown and other executives at SolarWinds prepared Form 8-K filings disclosing the event.[11] On October 30, 2023, the SEC brought securities fraud claims against SolarWinds and Brown based on alleged material omissions and misstatements in disclosures that were made in public statements and in SEC filings both before and after the SUNBURST attack.[12]

On July 18, 2024, the court dismissed the SEC's claims in large part, holding that the SEC had sufficiently pled misrepresentation and scheme liability claims only as to a 2017 security statement that SolarWinds had posted on its website.[13] The court found that misrepresentations were sufficiently alleged as to at least two of SolarWinds' five cybersecurity practices. In particular, the court held that the company's representations about its access controls and password protection policies, "as pled, were materially misleading by a wide margin" because the company had held itself out as maintaining "sophisticated cybersecurity controls" and as "heeding industry best practices," when, in reality, the company "fell way short" on basic requirements for cybersecurity.[14]

The court dismissed the SEC's remaining claims against SolarWinds and Brown. The court found that pre-SUNBURST attack press releases and blog posts were non-actionable corporate puffery, as they contained generalized statements that did not "purport to describe SolarWinds' cybersecurity practices" at a detailed enough level that a reasonable investor could rely on them.[15] For example, the SEC had challenged statements such as Brown's statement in a 2020 blog post that SolarWinds "places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards."[16]

Claims based on SolarWinds' cybersecurity risk disclosures in SEC filings were also dismissed because the risk disclosures, when "[v]iewed in totality," were "sufficient to alert the investing public" about the nature and types of cyber risks that SolarWinds faced and the potential consequences that these risks carried for the company.[17] The court found that SolarWinds' risk disclosures were "comfortably aligned" in terms of their "breadth, specificity, and clarity" with other risk disclosures that courts have held to be sufficient and that the securities laws do not require risks to be "articulated with maximum specificity."[18] As to the Form 8-Ks that SolarWinds had filed after the SUNBURST attack, the court found that the SEC's allegations were overly dependent on the benefit of hindsight, noting that "perspective and context are critical."[19] According to the court, SolarWinds' Form 8-K disclosures were made with "appropriate gravity and detail," given that SolarWinds filed a Form 8-K regarding the

8 Opinion at 27.

9 *Id.* at 27–28.

10 *Id.* at 27–37.

11 *Id.* at 37–43.

12 *Id.* at 44, 46.

13 *Id.* at 3.

14 *Id.* at 52, 58.

15 *Id.* at 68.

16 *Id.* at 67.

17 *Id.* at 72.

18 *Id.* at 72–73.

19 *Id.* at 86.

incident "just two days after" a customer had reported it, and that SolarWinds' own understanding of the cyberattack was still "evolving."[20]

The court further found that the SEC's novel internal accounting controls claims failed because the relevant statute regulates financial accounting controls, not cybersecurity controls.[21] In the court's view, the text of the statute did not support its application to cybersecurity controls, and there was no legislative evidence that Congress intended it to reach cybersecurity.[22] Instead, the statute's internal accounting controls requirement was "properly read to require" an issuer to "accurately report, record, and reconcile *financial* transactions and events."[23] The court explained that adopting the SEC's broad interpretation of this statute would have "sweeping ramifications" and could not be "squared with the statutory text."[24]

Finally, the court held that the SEC's disclosure controls claim failed because SolarWinds had systems in place that would assist with the disclosure of cybersecurity risks, and SolarWinds' Incident Response Plan was sufficiently capable in both design and execution of identifying and reporting information that was required to be disclosed.[25] The court also noted that the SEC did not plead that there were deficiencies in the construction of SolarWinds' disclosure system or that it frequently resulted in errors.[26]

We will continue to monitor developments in this space and provide further updates as appropriate.

* * *

[20] Opinion at 86.

[21] *Id.* at 96–98, 102.

[22] *Id.* at 96–98.

[23] *Id.* at 98 (emphasis in original).

[24] *Id.* at 100.

[25] *Id.* at 103–105.

[26] *Id.* at 104.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

L. Rush Atkinson
+1-202-223-7473
ratkinson@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Joshua Hill Jr.
+1-628-432-5123
jhill@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Peter Carey
+1-202-223-7485
pcarey@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Associates Neil Chitrao, Anita Y. Liu and Natalie A. Reynolds contributed to this Client Memorandum.