JENNER&BLOCK

Takeaways from *SEC v. SolarWinds* Motion to Dismiss Hearing

Client Alerts

May 30, 2024
By: Shoba Pillay, Charles D. Riely, Andrew P. Csoros

The SEC's high-profile litigation against SolarWinds and its Chief Information Security Officer (CISO), Timothy Brown, reached a critical juncture on May 15, 2024, when the parties presented oral arguments before Judge Paul A. Engelmayer in the Southern District of New York on Defendants' motion to dismiss. This client alert discusses the key critiques of the SEC's approach, important developments in the litigation, and highlights from the motion to dismiss hearing.

Background

As we noted in our prior client alert, the SEC filed its initial complaint against SolarWinds and its CISO Brown in October 2023, alleging that Defendants misled the company's investors and customers by overstating the company's cybersecurity practices and concealing mounting cybersecurity risks between October 2018 and January 2021.

The SEC's complaint focused on SolarWinds' flagship network monitoring product, Orion, which purportedly had abilities ranging from reducing network outages to improving network performance. Orion was used by virtually all Fortune 500 companies and many US government agencies. The SEC alleged that SolarWinds overstated the strength of its cybersecurity practices and prevention measures, and then failed to tell the whole truth after learning of a massive breach regarding Orion that impacted many of its key customers.

Industry Criticisms of the SEC's Action Against SolarWinds and Its CISO

SEC v. SolarWinds is a first-of-its-kind action asserting fraud and internal controls charges against a company and its CISO, and the action reflects the SEC's most aggressive use of its powers to address a company's alleged misrepresentations related to cybersecurity risk or incidents. In response to the initial complaint, numerous industry groups publicly criticized various aspects of the SEC's novel approach to the litigation:

- The cybersecurity industry has criticized the SEC for naming a CISO (or any individual) as a defendant for their role in cybersecurity failures. Underscoring the significance of the SEC's decision to name Brown as a defendant, a group of current and former CISOs and cybersecurity

organizations filed an *amicus* brief warning that the SEC's claims were counterproductive on several policy levels, including because it could worsen critical shortages of cybersecurity professionals by creating fear of personal liability.[1]

- The SEC was similarly criticized for alleging that the "internal accounting controls" provisions of the Exchange Act apply to cybersecurity controls and suggesting that companies and individuals can be charged with a securities violation for failing to protect company assets from cybersecurity attacks. Section 13(b)(2)(B), which was enacted as part of the Foreign Corrupt Practices Act in response to concerns about bribery of foreign officials by US business interests, requires public companies to maintain internal accounting controls "sufficient to provide reasonable assurances that . . . access to assets is permitted only in accordance with management's general or specific authorization." In response to the SEC's inclusion of this claim, the US Chamber of Commerce and Business RoundTable filed an *amicus* brief arguing that cybersecurity controls are unrelated to the reliability of financial reporting for purposes of the statute and that the use of this charge would unfairly penalize companies that are victims of a cyberattack.[2]

- The SEC's action also elicited general industry criticism that requiring public companies to disclose cybersecurity weaknesses would be counterproductive. They argue that heightened public disclosure of security vulnerabilities could make companies more vulnerable to attack by calling hackers' attention to their cybersecurity weaknesses and could chill internal discussions and self-assessments of those weaknesses.

The SEC's Amended Complaint

On February 16, 2024, the SEC filed an amended complaint against SolarWinds and CISO Brown. In an effort to respond to key critiques of the action, the amended complaint added significant detail to the allegations supporting its fraud and internal controls charges.

Notable allegations include the following:

Cybersecurity Disclosures and Reporting. The amended complaint added details to show why the conduct at issue in this case warranted an enforcement action. As in the initial complaint, the SEC alleged that SolarWinds and Brown misled investors and customers by overstating the company's cybersecurity practices, concealing mounting cybersecurity risk before the Orion breach, and failing to tell the whole truth after the Orion breach, in violation of the antifraud provisions of the Securities Act of 1933 and the Securities Exchange Act of 1934 and the false reporting provisions of the Exchange Act.[3]

The SEC's amended complaint also asserted at the outset that "[t]his is not a case about isolated failures, attempts at compliance that were good but less than perfect, or the SEC seeking to impose its own set of specific cybersecurity protocols on SolarWinds or all public companies."[4]

The amended complaint then detailed the specific practices that SolarWinds and Brown "touted" that were allegedly misleading, including SolarWinds' creation of its products in a "secure development lifecycle [that] follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments.'"[5] The amended complaint also flagged SolarWinds' statements that its servers were "monitored for the detection and prevention of various network security threats"; that SolarWinds' "password policy covers all applicable information systems, applications, and databases [and we] enforce the use of complex passwords"; that SolarWinds had "[a]ccess controls to sensitive data in our databases, systems, and environments [that] are set on a need-to know / least privilege necessary basis"; and that SolarWinds overall complied with the National Institute of Standards and Technology (NIST) Framework for evaluating cybersecurity practices.[6] Many of these statements appeared in a "Security Statement" on SolarWinds' website that was purportedly authored by Brown.[7]

Internal Accounting Controls. The SEC also sought to defend their allegation that Defendants violated the internal accounting controls provision of the Exchange Act by failing to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances" to prevent unauthorized access of SolarWinds' assets—*i.e.*, its software code and technology infrastructure.[8]

The SEC's amended complaint expounded on this novel charge, explaining that "[t]he cybersecurity controls at issue here were 'internal accounting controls' in that they were plans, procedures, and records of SolarWinds concerned with the safeguarding of corporate assets. Cybersecurity policies must be designed and implemented to provide shareholders with reasonable assurances that access to corporate assets—including technology assets, computer code and software for distribution to customers—are limited to authorized users, and thus support the twin goals of corporate accountability and management stewardship over corporate assets underlying Rule 13(b)(2)(B)."[9]

The Motion to Dismiss Hearing

After Defendants filed a motion to dismiss the SEC's amended complaint, the Court held an oral argument that focused on key issues in the case.[10]

Scienter premised on Brown's state of mind vs. knowledge of other individuals within the company. The SEC identified an expansive set of alleged false statements, including in its SEC filings, a Security Statement on SolarWinds' website, and interviews and blogposts by Brown.

At the hearing, the SEC sought to defend their allegation that Defendants acted with scienter with two key arguments. First, the SEC alleged that Brown had scienter because he portrayed SolarWinds as a cybersecurity leader—through the Security Statement, presentations, podcasts, and press releases—when he knew the opposite was true. The SEC argued that, although Brown did not sign

the risk factor at issue, there was sufficient "connective tissue" between the person with scienter (Brown) and the persons who made the statements (senior executives who relied on Brown's representations and subcertifications).[11] Second, the SEC argued in the alternative that, even if not Brown, someone at the company must have had scienter based on the reality on the ground.[12] To support this argument, the SEC argued at the pleadings stage, it was not required to identify an individual with scienter when the statements were "so divorced from reality that somebody must have had scienter."[13]

Duty to make and/or update specific risk disclosures keyed to SolarWinds' business. The Court focused on the interplay between the cybersecurity risk factor disclosures in SolarWinds' SEC filings and the Security Statement on SolarWinds' website. Among other things, the Court probed whether the company's risk factors could be considered too "generic" and "terribly out of date" once Orion customers had reported network breaches in May 2020 and October 2020.[14] The Court also emphasized that "[t]his is not a generic cybersecurity risk that any company in America that sells pizzas or TVs or cars might have. *This is a cybersecurity risk involving a company that sells cybersecurity, that sells software, and the issue here is not do you have to disclose incremental problems with your alarm system, it's at what point do we have to disclose the fact that our flagship product might be corrupted."* [15]

Statements on SolarWinds' website indicating that the company was "following" the NIST Framework. In addition to SolarWinds' risk disclosures, the SEC's fraud claims focused on the strength of SolarWinds' network defenses, including that the company followed the NIST Framework, which the SEC alleged was materially false because they did not reveal how SolarWinds fared in internal assessments using the NIST Framework.

In response to arguments that the NIST Framework is a self-evaluation framework, the SEC explained that it is "a materially misleading omission to claim to follow NIST without revealing how poor they score on certain critical components of it."[16] Nevertheless, the Court observed that "within the range of the allegations, this is not [the SEC's] strongest one."[17]

The CISO's Subcertifications. The SEC focused on Brown's signed subcertifications, arguing that Brown's subcertifications misled senior executives regarding the health of SolarWinds cybersecurity environment. In response to the Court's questioning, the SEC identified Brown's specific subcertification, noting that "Brown signed subcertifications relied on by the senior executives *confirming that all discrepancies, issues, or weaknesses had been disclosed to the executives responsible for the security filings.*"[18] In essence, the SEC's subcertification theory concerns Brown's failure to elevate information about cybersecurity weaknesses in light of his subcertification.

Internal Accounting Controls. The Court challenged the SEC's interpretation of Section 13(b)(2)(B) of the Exchange Act.

The Court questioned both whether Section 13(b)(2)(B) went beyond tangible, countable assets for accurate financial reporting to include software assets, and whether SolarWinds' software code was "lost." As part of the discussion, the Court noted, "SolarWinds still has its software code. What it has sold to its customer has been compromised, but back at the shop they still have their software code."[19]

Key Takeaways

- ***SEC v. SolarWinds* is a bellwether case for how the SEC will approach cybersecurity enforcement.** As noted above, the SEC asserted first-of-its-kind theories and charges in the initial complaint, and then bolstered its claims in the amended complaint in the face of industry criticism. If successful, the SEC is likely to bring additional disclosure actions against public companies and their CISOs that assert fraud and internal accounting controls charges in the wake of a breach.

- **Companies and CISOs need to be cautious in how they describe their cybersecurity practices and risks in light of an evolving threat landscape.** The motion to dismiss hearing portended a possibility that many of the alleged false statements—particularly those contained in SolarWinds' Security Statement—may survive the pleadings stage. Companies should consult with counsel who are familiar with both cyber-risk management and SEC enforcement to ensure that their disclosures minimize potential exposure in light of SolarWinds.

- **Companies and their CISOs need to be aligned on a CISO's disclosure and controls obligations.** The SEC's case—and the motion to dismiss hearing—centered on Brown's involvement in SolarWinds' Security Statement posted on its website, SEC filings, and signed subcertifications. Much of the discussion at oral argument probed Brown's participation in these statements, as well as his alleged failure to provide material information to other executives responsible for making security disclosures, even if it was not entirely clear whether, and to what extent, Brown had disclosure obligations within the company.

While the result of the motion is far from clear, the developments to date reveal that companies and CISOs should continue to exercise caution (and work with counsel) to ensure that they meet their disclosure and control obligations.

Footnotes

[1] Brief of Chief Information Security Officers & Cybersecurity Organizations as Amici Curiae Supporting Defendants, *SEC v. SolarWinds* & Brown, No. 1:23-cv-09518 (S.D.N.Y. Feb. 2, 2024), ECF No. 70-1.

[2] Brief of US Chamber of Commerce & Business Roundtable as Amici Curiae Supporting Defendants, *SEC v. SolarWinds* & Brown, No. 1:23-cv-09518 (S.D.N.Y. Feb. 2, 2024), ECF No. 68-1.

[3] Amended Complaint ¶¶ 6–9, *SEC v. SolarWinds* & Brown, No. 1:23-cv-09518 (S.D.N.Y. Feb. 16, 2024), ECF No. 85.

[4] *Id.* at ¶ 2.

[5] *Id.* at ¶ 7.

[6] *Id.* at ¶¶ 7, 72, 179.

[7] *See id.* at ¶¶ 56–61.

[8] Id. at ¶ 320.

[9] Id. at ¶ 321.

[10] Motion to Dismiss, *SEC v. SolarWinds* & Brown, No. 1:23-cv-09518 (S.D.N.Y. March 22, 2024), ECF No. 89.

[11] Transcript of Oral Argument at 50–51, *SEC v. SolarWinds* & Brown, No. 1:23-cv-09518 (S.D.N.Y. May 15, 2024).

[12] *Id.*

[13] *Id.* at 64

[14] *Id.* at 5–6.

[15] *Id.* at 11.

[16] *Id.* at 44–45.

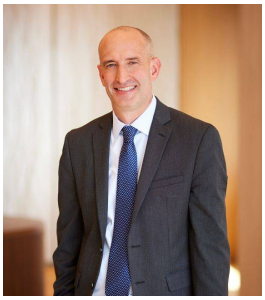
[17] *Id.* at 31.

[18] *Id.* at 51–52.

[19] *Id.* at 77–78.

Related Attorneys

Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605



Charles D. Riely
Partner
criely@jenner.com
+1 212 891 1686

Andrew P. Csoros
Special Counsel
acsoros@jenner.com
+1 312 840 7533

Related Capabilities

Data Privacy and Cybersecurity

Investigations, Compliance, and Defense

Investor and Securities Litigation

the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with SRA number 615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed →