Client Alert | **Newsflash** | US Public Company Advisory / White Collar/Investigations / Data, Privacy & Cybersecurity

Judge Rejects SEC's Aggressive Approach to Cybersecurity Enforcement

July 29, 2024

On July 18, 2024, a New York federal judge dismissed most of the U.S. Securities and Exchange Commission's ("SEC") claims against SolarWinds Corp. ("SolarWinds" or the "Company") and its Chief Information Security Officer ("CISO"), Timothy G. Brown, in connection with the Company's cybersecurity practice. The ruling dismissed all allegations related to SolarWinds' pre-SUNBURST cyberattack risk factor disclosure and post-SUNBURST Form 8-K disclosure, as well as claims concerning SolarWinds' internal accounting and disclosure controls. The Court, however, allowed the SEC to move forward with its claim that SolarWinds committed securities fraud due to misrepresentations on the Company's website regarding cybersecurity vulnerabilities.

This decision is a significant blow to the SEC's aggressive approach to cybersecurity enforcement. Not only did the Court find the SEC failed to allege intentional fraud based on the disclosure in the Company's SEC filings, but the Court also found the SEC cannot use its internal accounting controls provision to regulate cybersecurity controls.

Background

SolarWinds, a NYSE-listed public company that went public in 2018, develops software for companies and government agencies to manage their information technology infrastructure. In December 2020, it was publicized that SolarWinds had been the victim of the "SUNBURST" cyberattack, which is believed to have been conducted by Russian state-sponsored hackers.[1]

On October 30, 2023, the SEC filed its Complaint in the Southern District of New York, alleging that SolarWinds and its CISO, Brown, violated the antifraud provisions of the Securities Act of 1933 and the Securities Exchange Act of 1934 ("Exchange Act"). The Complaint also alleged that SolarWinds violated reporting, internal accounting control, and disclosure controls provisions of the Exchange Act; and that Brown aided and abetted the Company's violations. The SEC alleged that SolarWinds and Brown defrauded investors by overstating the Company's cybersecurity practices and understating or failing to disclose known cybersecurity risks. For more details on the SEC's claims, see our prior article at: White & Case Client Alert "The SEC's Charges Against SolarWinds and its

[1] See David E. Sanger et. al, Scope of Russian Hacking Becomes Clear: Multiple US Agencies Were Hit, (Dec. 14, 2020), https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

Chief Information Security Officer Provide Important Cybersecurity Lessons for Public Companies" (November 2023).[2]

Internal Accounting Controls Claim

Among the claims dismissed by the Court was the SEC's allegation that SolarWinds failed to "devise and maintain appropriate 'internal accounting controls'" sufficient to protect its most critical assets from unauthorized access, violating Section 13(b)(2)(B)(iii) of the Exchange Act.[3] Section 13(b)(2)(B)(iii) requires companies to have "internal accounting controls" sufficient to assure that companies' assets are accessed only with management's authorization. Relying on this provision, the SEC argued that SolarWinds' source code, databases, and products were its most vital assets.[4] The SEC alleged that because of the Company's poor access controls, weak internal password polices, and VPN security gaps, hackers were able to access SolarWinds' assets without management's authorization.[5] SolarWinds countered that as a matter of statutory construction, "internal accounting controls" cannot reasonably be interpreted to cover a company's cybersecurity controls.[6] The Court agreed, finding the SEC's reading of the provision to be "not tenable" because the term "internal accounting controls" refers to a company's "financial accounting," which is "one element of a control system implemented to safeguard assets and promote reliable financial records."[7] As "internal accounting controls" are controls to ensure companies "accurately report, record, and reconcile *financial* transactions and events," cybersecurity controls do not reasonably fit within this term."[8] The Court did not deny the vital importance of cybersecurity controls.[9] However, the Court found, the SEC's interpretation would mean that Section 13(b)(2)(B)(iii) would "broadly cover all systems public companies use to safeguard their valuable assets," and would have "sweeping ramifications" as to how public companies are regulated.[10]

Disclosure Controls and Procedures Claim

The Court also dismissed the SEC's allegations that SolarWinds violated Rule 13a-15(a) by failing to "maintain disclosure controls and procedures."[11] The Court found that the Company had a system in place to facilitate timely and accurate disclosure.[12] The mere mischaracterization of two incidents in the Company's incident response plan, without more, did not amount to deficient disclosure controls, as "errors happen without systemic deficiencies."[13]

SEC Filing Disclosure Claims

The Court also dismissed all the SEC's charges related to SolarWinds' allegedly inadequate cybersecurity risk factor disclosures prior to the 2020 SUNBURST cyberattack, as well as the Form 8-K disclosure that reported on the SUNBURST cyberattack.[14]

---

[2] White & Case Client Alert "The SEC's Charges Against SolarWinds and its Chief Information Security Officer Provide Important Cybersecurity Lessons for Public Companies" (Nov. 14, 2023), https://www.whitecase.com/insight-alert/secs-charges-against-solarwinds-and-its-chief-information-security-officer-provide.

[3] *SEC v. SolarWinds Corp.*, No. 1:23-cv-9518 (S.D.N.Y. July 18, 2024), at 94, 102.

[4] *Id*. at 94.

[5] *Id.* at 94–95.

[6] *Id.* at 95.

[7] *Id.* at 95–96, 98 (internal quotations omitted).

[8] *Id.* at 98.

[9] *Id.*

[10] *Id.* at 100.

[11] *Id.* at 102.

[12] *Id.* at 103–04.

[13] *Id.*

[14] *Id.* at 69–72, 94.

In its Complaint, the SEC alleged that SolarWinds' risk factor disclosure was "unacceptably boilerplate and generic" and inadequate given the Company's internal recognition that its security systems were faulty.[15] The disclosure started with allegedly generic disclosure that SolarWinds "could suffer a loss of revenue and increased costs, exposure to significant liability, reputational harm and other serious negative consequences" if the Company was subject to cyberattacks against its systems or its products.[16] But the disclosure went further to list specific risks SolarWinds faced given its business model, which included the Company's vulnerability to "damage or interruption" from hackers and that "SolarWinds might prove unable to anticipate, prevent, or detect such attacks."[17] The disclosure also alerted investors to the damaging consequences to the Company as a result of a security breach.[18] The Court found that the Company's risk factor disclosure was sufficient to alert investors about the "types and nature of the cybersecurity risks SolarWinds faced and the grave potential consequences" to the Company.[19] Although some of the disclosure was "formulaic," the Court found that "viewed in totality," the disclosure provided acceptable "breadth, specificity, and clarity."[20]

The SEC also alleged that the risk disclosure was inadequate because SolarWinds did not update it after learning of two cyber incidents from customers.[21] The Court found that SolarWinds did not have the duty to update its cybersecurity risk disclosure concerning the two incidents in light of the Company's already fulsome disclosure because the adequacy of the Company's "pre-SUNBURST risk disclosure must be evaluated based on the information the [C]ompany had in real time and the conclusion it reasonably drew from that information."[22] The Court found that, at the time the Company made the disclosure, it did not have enough information about the two incidents to "reliably draw [a] conclusion."[23]

Regarding SolarWinds' Form 8-K disclosure following the SUNBURST cyberattack, the Court ruled that the SEC failed to plausibly allege actionable deficiencies in SolarWinds' disclosures because those allegations "impermissibly rely on hindsight and speculation."[24] The Court found that "[t]he disclosure was made at a time when SolarWinds was at an early stage of its investigation, and when its understanding of that attack was evolving."[25] The Court further found that the first Form 8-K disclosure was promptly made just two days after the Company's CEO was updated on the vulnerability in the Company's product resulting from the attack.[26] Considering the short turnaround, the Court concluded that the disclosure fairly captured the known facts at the time as to the severity of the attack and the potential for grave harm as a result.[27]

Claims Against the CISO

The Court also dismissed the SEC's claims against the CISO, Brown, over the disclosure made in the Company's SEC filings, because the SEC fell far short of pleading with particularity the CISO's scienter through "conscious behavior," and it did not "attempt to plead his scienter based on motive and opportunity."[28] The Court found that Brown did not deliberately withhold information from the persons responsible for creating risk disclosure, and did not have a duty to disclose additional information to Company officials given the facts available at the time.[29] As

[15] *Id.* at 71.
[16] *Id*.
[17] *Id.*
[18] *Id.* at 72.
[19] *Id.*
[20] *Id.*
[21] *Id.* at 74.
[22] *Id.* at 75–76.
[23] *Id.* at 76.
[24] *Id.* at 3.
[25] *Id.* at 86.
[26] *Id.*
[27] *Id.* at 86–90.
[28] *Id.* at 80.
[29] *Id.* at 81, 93.

such, the Court found that Brown's conduct was not "highly unreasonable" or "an extreme departure from the standards of ordinary care."[30]

Security Statement Disclosure Claims

The Court, however, did not dismiss the SEC's case entirely. The Court sustained the SEC's claim that SolarWinds' Security Statement, which was posted on the Company's website, misrepresented to the public the adequacy of its cybersecurity practices even though the Company knew the vulnerabilities of such practices, which included poor access control and password protection.[31] The Court found that "[g]iven the centrality of cybersecurity to SolarWinds' business model as a company pitching sophisticated software products to customers for whom computer security was paramount these misrepresentations were undeniably material," thus constituting a sustained claim of a public misrepresentation.[32] The Court also upheld claims over the CISO, Brown's, role in the SolarWinds' allegedly false and misleading representations in the Security Statement about the Company's cybersecurity practice.[33]

Key Takeaways

- **The case represents a setback for the SEC in its aggressive enforcement efforts.** Recently, the SEC has started to expansively apply Section 13(b)(2)(B)'s "internal accounting controls" provision to compel public companies to adopt policies and practices that do not directly involve the financial statements.[34] Just one month prior to the SolarWinds opinion, the SEC settled similar internal accounting controls charges, finding that R.R. Donnelly & Sons, Co. failed to maintain adequate cybersecurity controls.[35] The SEC had also previously brought similar charges for an issuer's alleged failure to maintain internal controls to adequately monitor its stock repurchase plans.[36] The SolarWinds decision reflects judicial acknowledgement that there are limits on the application of Section 13(b)(2)(B)'s accounting controls provision. The implications of the dismissal of the internal accounting controls claims remain uncertain, however, as the SEC may continue to attempt to apply the internal accounting controls provision to a broad range of public company practices.

- **Clear, specific, and broad-based risk factor disclosure carried the day.** The case provides guidance as to the relevant disclosure standards for companies' cyber risk factor and 8K event disclosure. Vague, boilerplate statements as to risks and consequences are inadequate. Risk factor disclosure should sufficiently alert investors about the types and nature of the specific cybersecurity risks faced, taking into account the specific business model, and the grave potential consequences to the company stemming from a cyber incident. Although the SEC does not require a company to disclose incidents for which it does not have sufficient information to reliably draw a conclusion, the total impact of a company's cybersecurity practices, remedial efforts, identified risks and known threats or attacks needs to be evaluated collectively when crafting a disclosure, with all information available at the time, rather than looking at isolated incidents individually. Particular attention should be paid to disclosure of cybersecurity

[30] *Id.* at 81–82, 92–93.

[31] *Id.* at 50–67.

[32] *Id.* at 56.

[33] *Id.* at 65.

[34] *See* Statement of Commissioners Hester M. Peirce and Mark T. Uyeda, *Hey, look, there's a hoof cleaner! Statement on R.R. Donnelley & Sons, Co.* (June 18, 2024), https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-rr-donnelley-061824#_ftn1.

[35] R.R. Donnelley & Sons, Co., Rel. No. 34-100365, (June 18, 2024), https://www.sec.gov/files/litigation/admin/2024/34-100365.pdf.

[36] *See* Statement of Commissioners Hester M. Peirce and Mark T. Uyeda, *The SEC's Swiss Army Statute: Statement on Charter Communications, Inc.* (Nov. 14, 2023), https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-charter-communications-111423; *see also* Statement of Commissioners Hester M. Peirce and Mark T. Uyeda, *Statement of Commissioners Hester M. Peirce and Elad L. Roisman - Andeavor LLC* (Nov. 13, 2020), https://www.sec.gov/newsroom/speeches-statements/peirce-roisman-andeavor-2020-11-13.

risks and issues relating to "crown jewel" or flagship products or services that account for a significant portion of a company's revenues.

- **Individuals may be charged with fraud in the disclosure context, but "scienter" must be present.** The fraud and aiding and abetting claims against the SolarWinds CISO highlight the imperative for public company CISOs and other officers to communicate vulnerabilities to senior executives, participate in the disclosure committee process and ensure that public disclosures are specific, detailed, timely and consistent with internal communications. "Scienter" is likely not to be found if a CISO does not deliberately withhold information from the persons responsible for creating the disclosure, and if there is no clear duty to disclose particular cybersecurity incidents given the facts available at the time.
- **Statements on websites, such as security statements, are fair game for claims of misrepresentation.** This decision underscores the necessity for public companies to review and scrutinize all public disclosures regarding their cybersecurity practices. The SEC will consider all public disclosures, not just SEC filings, when assessing compliance. This includes a company's privacy policy or other online representations regarding the company's cybersecurity practices that appear on a company's website. As such, companies need to ensure that their representations about the adequacy and scope of their cybersecurity programs are internally consistent, accurate, and transparent.
- **Cyber disclosure remains an important area that companies need to focus on.** This requires appropriate controls, adequate governance, determination of materiality and assessment of the sufficiency of the disclosure as a whole. Boards of directors and management teams should be kept informed and should address any identified issues, and design and implement controls and procedures to ensure that cybersecurity incidents and risks are identified and appropriately escalated to senior management. This also includes maintaining a written incident response plan that formalizes and evidences a company's systematic approach to responding to a cyber incident and facilitates the appropriate and timely reporting to the SEC or other regulators.

Authors: Tami Stark, Maia Gez, F. Paul Pittman, Michelle Rutta, Shuhang Liu

In this publication, White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case LLP, a limited liability partnership incorporated under English law and all other affiliated partnerships, companies and entities.

This publication is prepared for the general information of our clients and other interested persons. It is not, and does not attempt to be, comprehensive in nature. Due to the general nature of its content, it should not be regarded as legal advice.

© 2024 White & Case LLP