The Computer & Internet Lawyer

Volume 41 ▲ Number 9 ▲ October 2024

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Court Dismisses Securities and Exchange Commission's Novel Cybersecurity Claim Against SolarWinds

By Adam S. Aderton, Daniel K. Alvarez, Laura E. Jehl and Baldwin Jahi Beal

The Securities and Exchange Commission's (SEC) efforts to leverage internal accounting controls provisions to regulate issuer cybersecurity policies hit a major obstacle recently when U.S. District Judge Paul Engelmayer of the Southern District of New York dismissed substantial portions of the SEC's claims against SolarWinds Corp.[1] Most notably, the court dismissed the SEC's claims that SolarWinds' alleged cybersecurity deficiencies violated the accounting controls requirements of Section 13(b)(2)(B) of the Securities Exchange Act of 1934 (Exchange Act) – a provision that requires companies to maintain "a system of internal accounting controls sufficient to provide reasonable assurances that . . . access to assets is permitted only in accordance with management's general or specific authorization." The court found that the SEC's application of this requirement to cybersecurity activities was not tenable as a matter of statutory construction: "[F]ailure to detect a cybersecurity deficiency (e.g., poorly chosen passwords) cannot reasonably be termed an *accounting* problem."[2]

The authors, attorneys with Willkie Farr & Gallagher LLP, may be contacted at aaderton@willkie.com, dalvarez@willkie.com, ljehl@willkie.com and bbeal@willkie.com, respectively.

THE SEC'S FIRST CLAIM OF INTERNAL ACCOUNTING CONTROLS VIOLATION IN A CYBERSECURITY MATTER

On December 14 and 17, 2020, SolarWinds, a U.S. software company whose products are widely used to manage IT networks, systems, and infrastructure, disclosed in SEC filings that a targeted cyberattack had inserted a vulnerability into its centralized IT monitoring and management software, Orion. SolarWinds stated that up to 18,000 customer-installed Orion products might be affected by the vulnerability.

Three years later, on October 30, 2023, the SEC brought an enforcement action against SolarWinds, alleging violations of multiple provisions of the federal securities laws. First, the SEC asserted a fraud claim based on allegations that the company (1) misleadingly touted its cybersecurity practices and products, including its flagship "Orion" software platform, and understated its cybersecurity risks, and (2) misled the investing public about a series of cyberattacks

known as SUNBURST.[3] The SEC also included the novel claim that SolarWinds' cybersecurity deficiencies were actionable under Section 13(b)(2)(B)(iii) internal accounting controls provisions because (1) the company's source code, databases, and products were its most vital assets, and (2) as a result of its poor access controls, weak internal password policies, and virtual private network (VPN) security gaps, the company failed to limit access to these "only in accordance with management's general or specific authorization," enabling access by external attackers.[4]

THE COURT'S ANALYSIS OF THE INTERNAL ACCOUNTING CLAIM IN THE SOLARWINDS CASE

The SolarWinds Court found that Section 13(b)(2)(B) cannot reasonably be interpreted to cover a company's cybersecurity controls such as its password and VPN protocols. The court focused on the text of Section 13(b)(2)(B)(iii), which requires that public companies "devise and maintain a system of *internal accounting controls* sufficient to provide reasonable assurances that . . . access to *assets* is permitted only in accordance with management's general or specific authorization." The court reasoned that the provision on its face applies only to a company's "system of internal *accounting* controls." For the SEC's claim to survive dismissal, that provision must be construed to extend to an issuer's cybersecurity controls.

The court found that, as a matter of statutory construction, the SEC's reading of Section 13(b)(2)(B) was not tenable because:

- The text of the statute strongly supports that the term "system of internal accounting controls" refers to a company's *financial accounting*. The term "accounting" is defined in Merriam-Webster Dictionary as "the system of recording and summarizing *business and financial* transactions and analyzing, verifying, and reporting the results." In addition, the SEC did not cite any dictionary definition of *accounting* favoring its construction.

- The related terms that Congress used in Section 13(b)(2)(B) – such as "transactions," "preparation of financial statements," "generally accepted accounting principles," and "books and records" – are uniformly consistent with the idea of "accounting" as financial accounting.

- There is no evidence that Congress intended its use of a "system of internal accounting controls" to include cybersecurity controls, and the statute was enacted in 1977 before cybersecurity was a relevant issue for businesses.

- Other courts have consistently construed the term "internal accounting controls" to address only financial accounting.

MOVING FORWARD

While the decision was focused primarily on the SEC's allegations against SolarWinds, it is likely to have broader implications for both the SEC and public issuers. Just recently, the SEC announced a $2.1 million civil penalty stemming f rom charges that a second public company, R.R. Donnelley & Sons Company (RRD), failed to execute a timely and effective response to a ransomware attack in late 2021 because of its disclosure and internal control deficiencies.[5] As with SolarWinds, the SEC alleged that RRD's cybersecurity deficiencies amounted to a failure to appropriately manage its internal accounting controls under Section 13(b)(2)(B). The SEC also alleged that RRD violated Rule 13a-15(a), which requires issuers to maintain disclosure controls and procedures. In that situation, RRD chose to settle with the SEC rather than fight the charges. In light of the outcome in SolarWinds, other parties in similar situations are now likely reconsidering whether and how to respond to analogous SEC allegations.[6]

The court's dismissal of the SEC's internal accounting and disclosure controls and procedures claims as "ill-pled" likely spells at least a reprieve from the SEC's efforts to significantly expand the scope of Section 13(b)(2)(B), although the agency may appeal. Public companies should nevertheless ensure that their cybersecurity practices are comprehensive and adequate, and that they are in compliance with other cyber-facing SEC requirements, including prompt notification of any material cyber incident.

Notes

1. Securities and Exchange Commission v. SolarWinds Corp., Case 1:23-cv-09518 (S.D.N.Y. July 18, 2024).
2. Id. at 98.
3. The SEC also asserted the same fraud claim against SolarWinds Chief Information Security Officer, Timothy G. Brown. Brown is the first corporate executive to face charges in a cybersecurity disclosure case. In the analysis of fraud claims against SolarWinds and the CISO, the court distinguished between "pre-SUNBURST" and "post-SUNBURST" disclosures. Pre-SUNBURST disclosures consist of the company's Security Statement; statements made in connection with the October 2018 Initial Public Offering; and 2018-20 statements made in press releases, blog posts, podcasts, and presentations. While

post-SUNBURST disclosures are the company's December 14 and 17, 2020 Form 8-Ks, in which it disclosed the SUNBURST attack. The court found that the Security Statement contained misrepresentations and sustained the SEC's claims of securities fraud in regard to the statement. However, the court dismissed fraud claims pertaining to the remaining disclosures.

4. The SEC also brought a claim against SolarWinds under Exchange Act Rule 13a-15(a) which requires companies to "maintain disclosure controls and procedures." In particular, the SEC alleged that, prior to SUNBURST, two cybersecurity incidents and a VPN vulnerability were not appropriately escalated to SolarWinds' executives. The court dismissed this claim, noting that the SEC did not allege that SolarWinds lacked a system of controls to facilitate disclosure of potentially material cybersecurity risks, nor did it plead any deficiency in the construction of the system.
5. Press Release. SEC Charges R.R. Donnelley & Sons Co. with Cybersecurity-Related Controls Violations, U.S. SECURITIES AND EXCHANGE COMMISSION (June 18, 2024) available at https://www.sec.gov/news/press-release/2024-75; SEC Administrative Proceeding, In the Matter of R.R. Donnelley & Sons Co., Release No. 100365, File No. 3-21969 U.S. SECURITIES AND EXCHANGE COMMISSION (June 18, 2024).
6. The court's analysis on internal accounting controls parallels the framework of an earlier dissent by two SEC Commissioners, Hester Peirce and Mark Uyeda, who issued a joint dissenting statement in the RRD enforcement matter to disagree with the SEC's interpretation of Section 13(b)(2)(B) and argue that the expansive interpretation of what constitutes an "asset" under the provision exceeds the limits of the Exchange Act. Statement of Commissioners Hester M. Peirce and Mark T. Uyeda., Hey, Look, There's a Hoof Cleaner! Statement on R.R. Donnelley & Sons Co., U.S. SECURITIES AND EXCHANGE COMMISSION (June 18, 2024) available at https://www.sec.gov/news/statement/peirce-uyeda-statement-rr-donnelley-061824?utm_medium=email&utm_source=govdelivery.