August 1, 2024

Judge Curtails SEC's Cybersecurity Claims Against SolarWinds, Setting Precedent for Future Cases

By Kit Addleman, Kurt Gottschall, Tim Newman and Payton Roberts

On July 18, 2024, a federal judge in the Southern District New York dismissed a large portion of the SEC's cybersecurity enforcement lawsuit against SolarWinds and its Chief Information Security Officer (CISO). In a notable setback to the SEC, the court rejected the agency's novel theories that the company's cybersecurity failures and subsequent disclosures regarding the breach violated the internal *accounting* controls and disclosure controls provisions of the federal securities laws.[1] The decision provides needed clarity around the scope of the agency's enforcement authority in the realm of cybersecurity.

Background

In December 2020, SolarWinds announced that an unknown threat actor had compromised its flagship software product, Orion.[2] The cyber incident, later dubbed SUNBURST, involved a "highly sophisticated, targeted and manual supply chain attack by an outside nation state."[3]

The compromise of the SolarWinds Orion product was particularly significant because the software was used by thousands of government and private sector customers to monitor their networks and other IT systems.[4] Subsequent forensic analysis determined that the compromise of Orion enabled an extensive series of cyberattacks on SolarWinds customers that occurred between January 2019 and November 2020.[5] According to the SEC, hackers infiltrated SolarWinds' corporate VPN, conducted reconnaissance, collected data, identified vulnerabilities, and harvested credentials of SolarWinds employees.[6] The hackers then attempted to push malware out to SolarWinds customers and infiltrate their networks.[7]

---

[1] *SEC v. SolarWinds Corp.*, No. 1:23-CV-09518 (S.D.N.Y. July 18, 2024).

[2] SolarWinds Corp., Current Report (Form 8-K) (Dec. 14, 2020) ("Form 8-K"), available at https://www.sec.gov/ix?doc=/Archives/edgar/data/0001739942/000162828020017451/swi-20201214.htm ("Dec. 14 Form 8-K").

[3] *Id.*

[4] Amended Complaint at ¶ 4, *SEC v. SolarWinds Corp.*, No. 1:23-CV-09518 (S.D.N.Y. July 18, 2024), ECF No. 85 (the "Amended Complaint").

[5] *Id.* at ¶¶ 254–55.

[6] *Id.* at ¶ 255.

[7] *Id.* at ¶ 258.

On October 30, 2023, the SEC sued SolarWinds and its CISO, alleging violations of the antifraud, internal accounting and disclosure controls provisions.[8]

The Court Rejected the SEC's Theory that SolarWinds Violated Internal Accounting Controls Requirements

In a theory that had not been litigated previously,[9] the SEC alleged that SolarWinds' cybersecurity failures amounted to a violation of Exchange Act Section 13(b)(2)(B), which requires public companies to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that . . . (iii) access to assets is permitted only in accordance with management's general or specific authorization. . . ."[10] The SEC asserted that "(1) the company's source code, databases, and products were its most vital assets, but (2) as a result of its poor access controls, weak internal password policies, and 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."[11]

The Court flatly rejected the SEC's theory. According to the Court, Section 13(b)(2)(B) only authorizes the SEC to exercise authority over internal *accounting* controls.[12] "[T]here is no evidence of any other sort that Congress intended its reference to 'a system of internal accounting controls' to reach cybersecurity controls."[13] The court reasoned that the statute was designed to regulate a company's controls related to its financial statements and accounting systems, which did not extend to all systems public companies use to safeguard assets.[14] The Court thus dismissed the SEC's claim that SolarWinds' cybersecurity failures violated internal *accounting* controls requirements.

---

[8] The original complaint was later amended on February 16, 2024. See Amended Complaint.

[9] In several settled actions, the SEC had signaled an aggressive interpretation of the scope of internal accounting controls violations. *See, e.g.*, Press Release, Charter Communications to Pay $25 Million Penalty for Stock Buyback Controls Violations (Nov. 14, 2023), available at https://www.sec.gov/news/press-release/2023-235 (finding in a settled action that the respondent had violated internal accounting control requirements by failing to ensure that certain stock buybacks complied with board authorizations, which required any buybacks to adhere to Rule 10b5-1); *see also*, Press Release, SEC Charges R.R. Donnelley & Sons Co. with Cybersecurity-Related Controls Violations (June 18, 2024), available at https://www.sec.gov/newsroom/press-releases/2024-75 (settling an internal accounting control claim under a finding that the company had failed to "devise and maintain a system of cybersecurity-related internal accounting controls" to ensure access to assets was permitted only by management's authorization).

[10] 15 U.S.C. § 78m(b)(2)(B) (otherwise known as Section 13(b)(2)(B) of the Exchange Act of 1934).

[11] Opinion at 94–95, *SEC v. SolarWinds Corp*., No. 1:23-CV-09518 (S.D.N.Y. July 18, 2024), ECF No. 125 (the "Opinion")..

[12] Opinion at 95–98.

[13] *Id.* at 97.

[14] *Id.* at 100.

The Court Also Dismissed The SEC's Disclosure Control Claim

The SEC also brought a disclosure control claim, alleging that SolarWinds failed to implement a system of internal controls designed to ensure the company complied with disclosure obligations under federal securities laws. The SEC specifically took issue with SolarWinds' misclassification of two SUNBURST-related incidents that resulted in them not being elevated for disclosure evaluation and the company's failure to elevate a security vulnerability for disclosure analysis.

The Court rejected the SEC's claims, finding that flaws in SolarWinds' actions relating to the incidents in question only were apparent with the benefit of hindsight. Regarding the incidents that were not elevated for review, the court found the SEC had not adequately pled that they had been misclassified based on the information available to SolarWinds at the time of the incidents. Only with the benefit of hindsight could the SEC allege that SolarWinds should have addressed the incidents differently. Moreover, in a ruling that likely will have broad applicability, the Court found that the alleged failure by SolarWinds to properly disclose a material incident or issue was not, by itself, an indication that SolarWinds' *system* of disclosure controls was deficient.

Court Allowed Certain Securities Fraud Claims to Proceed

The SEC also brought securities fraud claims against SolarWinds and its CISO based on alleged misstatements in a security statement posted to the company's website, its risk disclosures within its registration statement, press releases, podcasts, blogs, and SolarWinds' post-incident Forms 8-K. The court allowed the SEC's claims related to the security statement to proceed.

SolarWinds posted the "Security Statement" to its website in 2017 to inform customers of its "security infrastructure and practices."[15] The statement sought to address issues identified from customers' questionnaires, but was later described by one SolarWinds employee as "aspirational" and not necessarily accurate.[16] The SEC took issue with five particular statements within the Security Statement,[17] and claims related to the security statement's discussion of access controls and password protection policies survived dismissal.

Specifically, the Security Statement touted that "[r]ole based access controls are implemented for access to information systems."[18] It went on to say "[a]ccess controls to sensitive data in our databases, systems, and environments are set on a need-to-know/least privilege necessary basis."

However, the SEC pointed to internal presentations that the CISO helped draft to allege that these statements were materially misleading. For example, the internal presentations warned that too many employees had

---

[15] *Id.* at 6-7.

[16] *Id.*

[17] The five statements are: (1) SolarWinds compliance with National Institute of Standards and Technology Cybersecurity Framework for evaluating cybersecurity practices, (2) the use of secure developmental lifecycles to create its software products, (3) SolarWinds employment of network monitoring, (4) its strong password protections, and (5) SolarWinds sufficient access controls.

[18] Opinion at 53.

administrative level access, granting them access beyond what was necessary for their specific job functions. The court held this was sufficient to sustain the SEC's fraud claims regarding those statements.

The Security Statement also touted password protection policies, saying, "We require that authorized users be provisioned with unique account IDs. . . . Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords."[19]

However, the SEC pled that, as early as April 2017, employees had notified top executives that certain accounts had generic passwords, contrary to the representations made in the Security Statement, and the CISO had failed to correct the problem for years. The court thus allowed these claims to proceed.

The Court dismissed the rest of the SEC's claims that SolarWinds had misled investors. With respect to SolarWinds risk disclosures, the court acknowledged that they began with generic language, but found that they also listed specific risks faced by SolarWinds. Moreover, risk disclosures are not required to include "maximum specificity," according to the Court—just enough specificity to make them not misleading.[20]

Regarding SolarWinds' press releases, podcasts, and blog posts, the court ruled that the relevant statements were nothing more than "non-actionable corporate puffery, 'too general to cause a reasonable investor to rely upon them.'"[21]

Finally, with respect to the Forms 8-K SolarWinds filed after discovering SUNBURST, the Court emphasized that the first filing came 48 hours after SolarWinds' discovery of the incident, and the court reasoned that the report had sufficient gravity and detail for a report filed so quickly. While the first report did not directly link discovery to early warning signs, the court recognized that in the midst of an internal investigation, SolarWinds bluntly reported negative news regarding the incident and then, five days later, submitted another report with more detailed information. The court found that these two reports, given the circumstances, should not be subject to the SEC's speculation and hindsight and accordingly dismissed the SEC's claims.

Conclusion

Although the SEC was allowed to proceed on certain alleged misstatements to the public, the Court's ruling will provide public companies with compelling reasoning to defend against the SEC's expansive application of internal accounting controls and disclosure controls provisions to cybersecurity incidents.

The SolarWinds decision also will help public companies push back on SEC allegations of insufficiently detailed risk disclosures. The Court instead adopted a pragmatic approach that risk disclosures are not required to include "maximum specificity," and demonstrated that triers of fact recognize the difficulty and complexity of disclosing cyber incidents that are still under investigation.

---

[19] *Id.* at 56.

[20] *Id.* at 73.

[21] *Id.* at 68 (quoting *Loc. 134 IBEW Joint Pension Tr. of Chi. v. JP Morgan Chase Co.*, 553 F.3d 187, 206 (2d Cir. 2009)).

The SEC will continue to focus on cybersecurity as an important enforcement priority, but the SolarWinds decision provides much needed clarity around the scope of the SEC's authority to allege internal accounting controls and disclosure controls violations stemming from such incidents.