SULLIVAN & CROMWELL LLP

S&C memo

July 19, 2024

Court Dismisses Most of SEC's Claims Against SolarWinds and Its CISO

Ruling Curtails SEC's Authority to Bring "Internal Accounting Controls" Charges, and Rejects SEC's Claims that Company's Securities Filings Were False and Its Disclosure Controls Failed in Connection with a Cybersecurity Breach

SUMMARY

On July 18, 2024, Judge Paul A. Engelmayer of the United States District Court for the Southern District of New York granted, in large part, a motion by SolarWinds Corporation ("SolarWinds") and its Chief Information Security Officer ("CISO") to dismiss the fraud and internal controls charges brought against them by the Securities and Exchange Commission ("SEC") in the aftermath of a compromise of the company's software product that was disclosed in December 2020. The court allowed only the subset of claims alleging that the "Security Statement" on the company's website was materially false to survive.

The case, which has been closely followed, is the first in which the SEC has charged a CISO individually in connection with alleged cybersecurity violations and the first in which it has charged scienter-based securities fraud in connection with a cybersecurity breach. The case also represents a rare instance in which a company has challenged the SEC's expansive reading of its authority to charge a violation of the "internal accounting controls" provision of the Securities Exchange Act of 1934 (the "Exchange Act") based on an alleged failure of internal corporate controls—in this case, cybersecurity controls—not limited to financial accounting. The court's opinion has significant implications for public companies as they assess their cybersecurity risk management, governance and disclosure practices, and, beyond the cybersecurity context, in its finding that the SEC is not authorized to charge internal accounting controls violations that are not specifically tied to financial accounting controls.

BACKGROUND

As discussed in our earlier Memorandum to Clients, SolarWinds is a Texas-based company that produces software used for information technology management. Its flagship product, Orion, was used throughout the U.S. by governmental and private entities. On December 14, 2020, SolarWinds publicly disclosed that threat actors had inserted a vulnerability into certain versions of the Orion product.[1] In April 2021, the U.S. government attributed the attack to the Russian Foreign Intelligence Service, describing the exploitation of Orion as part of a "broad-scope cyber espionage campaign" that raised concerns for U.S. national security and public safety.[2]

On October 30, 2023, the SEC filed a complaint against SolarWinds and its CISO alleging that they misled investors and customers about known, material cybersecurity weaknesses and risks, including several that allegedly enabled the compromise. The SEC alleged that the defendants made materially false and misleading statements and omissions on SolarWinds' website and in its blog posts, press releases, initial registration statement ("Form S-1"), and quarterly and annual SEC reports before the incident, as well as in two current reports on Form 8-K in which SolarWinds disclosed the compromise. In an amended complaint filed in February 2024 ("Amended Complaint"), the SEC added factual detail in support of its allegation that the defendants knew that the company's statements about its security practices, as set forth in a "Security Statement" posted on the company's website, were false and misleading.

OPINION

A. Fraud and False and Misleading Statements

The court dismissed most of the SEC's securities fraud claims, including with respect to statements about the company's security made in press releases, blog posts, and podcasts, as well as in SolarWinds' securities filings. The court found, however, that the SEC adequately pleaded securities fraud claims premised on the "Security Statement" posted on SolarWinds' website during the relevant period.

Website "Security Statement". The SEC alleged that SolarWinds did not adhere to "various critical aspects of the Security Statement," including that SolarWinds adhered to the National Institute of Standards and Technology ("NIST") Cybersecurity Framework; that SolarWinds used a secure development lifecycle to develop its software;[3] and that the company employed adequate network monitoring, password protocols, and access controls. The SEC alleged that contrary to these "assurances," SolarWinds and its CISO knew that the company experienced "widespread and persistent failures" in each of these areas, which were important for the security of the company and its products.[4]

The court allowed the SEC's claims about each allegedly false part of the Security Statement to survive and limited its analysis in the opinion to the Security Statement's claims about the company's access controls and password protection policies. In doing so, it noted the following:

- "Blatantly contradict[ing]" the Security Statement's claims that the company strictly limited the scope of employees' access to its network, SolarWinds allegedly provided employees with administrative access (i.e., access to the entire network) on a "largely indiscriminate basis."[5] The SEC alleged that the CISO and the company were well aware that the company failed to limit access in the manner it claimed, and viewed the lack of restrictions as a serious deficiency. The court characterized the deficiency, as alleged, as "not only glaring" but also "long-standing, well-recognized within the company, and unrectified over time."[6] The court also stated that access controls deficiencies were "undeniably material," as alleged, given SolarWinds' business model, which centers on servicing customers "for whom computer security was paramount."[7]
- As to password policies, the court emphasized that the company and its CISO, as alleged, knew that the password policy described in the Security Statement was not enforced in practice. The court cited a variety of facts and examples alleged by the SEC to show that the company was aware that it maintained weak password controls including, among others, that a security researcher allegedly alerted the company and CISO that a password to one of the company's servers was publicly available, and that the password was "solarwinds123."[8]

The court noted that these alleged shortcomings may well be material for any company, but were "magnified for SolarWinds" given that cybersecurity was a "key attribute" of the company's products.[9] On the basis of the CISO's alleged knowledge of the falsity of the Security Statement in light of internal assessments and awareness within the company, the court found that the SEC had "easily plead[ed]" the CISO's scienter. Finally, the court rejected the defendants' argument that the Security Statement was directed at customers rather than investors, noting that it is "well established that false statements on public websites can sustain securities fraud liability."[10]

Press Releases, Blog Posts, and Podcasts. The court dismissed the SEC's claims that SolarWinds and its CISO made false and misleading statements in press releases, blog posts and podcasts touting the company's cybersecurity practices.[11] The court described these statements as "non-actionable corporate puffery," finding that "[n]one of these challenged materials purport to describe SolarWinds' cybersecurity practices or general business practices at the level of detail at which a reasonable investor would have relied on them in making investment decisions."[12]

Pre-incident Public Filings. The court dismissed the SEC's claims that SolarWinds' cybersecurity risk factor language, which was first included in its 2018 Form S-1 and remained unchanged in its periodic filings through 2020, materially understated the risks the company faced, which grew over time. The court first noted that risk factor language has been found actionable only in "the narrow circumstance" in which a matter described as a hypothetical risk had actually already materialized. Assuming *arguendo* that a risk factor could mislead an investor as to the nature of the risk, the court rejected the SEC's assertion that SolarWinds' risk factor language was "boilerplate" and limited to the "generic harms" that many companies face, finding instead that it set out "in stark and dire terms" the "unique risks" that SolarWinds faced as a cybersecurity company.[13] Quoting the disclosure language, the court noted that these risks included "the potential for . . . very damaging consequences" as a result of SolarWinds' heavy dependence on its technology infrastructure.[14] The court also noted that the Amended Complaint reflects that the CISO was responsible for drafting this "formidable list of cybersecurity risks."[15] The court concluded that the

cybersecurity risk factor "comfortably aligned with risk disclosures–of various types–that courts have upheld as adequate."[16]

Echoing concerns raised by SolarWinds and in *amicus* briefs submitted by former federal law enforcement officials in support of the company's motion to dismiss, the court also acknowledged that "spelling out a risk with maximal specificity," as the SEC appeared to be suggesting SolarWinds was required to do, "may backfire in various ways, including by arming malevolent actors with information to exploit" or by "misleading investors based on the formulation of the disclosure or the disclosure of other risks at a lesser level of specificity."[17] The court also rejected the SEC's argument that SolarWinds was obligated to update its disclosure language to account for two cybersecurity incidents reported by customers earlier in 2020 that were later found to be related to the larger compromise revealed in December 2020. The court focused on the fact that the company did not know at the time they occurred that the two incidents were significant or related to a "singular cyberattack, let alone [the] serious and pervasive" compromise that was later discovered.[18] The court cautioned that disclosure "must be evaluated based on the information the company had in real time and the conclusions it reasonably drew from that information" rather than "with the perspective of hindsight."[19]

December 2020 Form 8-K Filings. The court dismissed the SEC's claim that SolarWinds' filings on Form 8-K in December 2020, in which it detailed its understanding of the attack, were materially misleading in stating the company was investigating "whether, and to what extent,[20]" the vulnerability was exploited when, according to the SEC, the company knew the software had attempted to contact external servers as a result of the vulnerability that had been discovered. The court found that the company's statement was not incorrect or inconsistent with the software attempting to contact other servers, and that the disclosure clearly "captured the big picture" and "bluntly reported brutally bad news for SolarWinds." [21] The court detailed a litany of bad facts set forth in the company's Form 8-Ks, including that up to 18,000 customers were vulnerable to compromise by what appeared to be a nation-state actor.[22] Moreover, the court noted that "the market got the message," as SolarWinds' share price dropped over 16% on the date of the announcement and 8% more the next day.[23]

The court further emphasized SolarWinds issued the first of these disclosures "just two days" after learning of the compromise, and was at "early stage of its investigation, and when its understanding of that attack was evolving."[24]

B. Internal Accounting Controls

The Amended Complaint alleged that SolarWinds failed to maintain a system of internal accounting controls sufficient to provide reasonable assurances that access to company assets was permitted only in accordance with management's general or specific authorization, in violation of Section 13(b)(2)(B) of the Exchange Act, and that the CISO aided and abetted the violation. The SEC asserted that "SolarWinds' information technology network environment, source code, and products were among the Company's most

critical assets,"[25] and thus, when the company was hacked as a result of its allegedly deficient cybersecurity controls, the company violated Section 13(b)(2)(B).

The court dismissed the internal accounting controls claim, finding that the defendants were "clearly correct" that Section 13(b)(2)(B) "does not govern *every internal system* a public company uses to guard against unauthorized access to its assets," but is limited to financial accounting controls.[26] The court observed the significant implications of the SEC's claim to the contrary on the scope of the agency's authority to assert violations of the statute:

> The SEC's rationale, under which the statute must be construed to broadly cover all systems public companies use to safeguard their valuable assets, would have sweeping ramifications. It could empower the agency to regulate background checks used in hiring nighttime security guards, the selection of padlocks for storage sheds, safety measures at water parks on whose reliability the asset of customer goodwill depended, and the lengths and configurations of passwords required to access company computers.[27]

The court found that Section 13(b)(2)(B) is properly read to require an issuer to "accurately report, record, and reconcile financial transactions and events," and cannot be interpreted to include cybersecurity controls.[28] The court pointed to the statutory language indicating that the provision is limited to "accounting" controls and suggested that the term "assets" has the limited meaning it is given in the financial accounting context. The court also pointed to the purpose of the statute's enactment as part of the Foreign Corrupt Practices Act to ensure transactions "are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles," and the legislative history of the provision, which states that the definitions and objectives contained in the provision are taken from "'the authoritative accounting literature.'"[29] The court also observed that the few cases that have construed Section 13(b)(2)(B) have consistently interpreted it to address financial accounting. The court's reasoning largely tracked the arguments set forth in an *amicus* brief submitted by Sullivan & Cromwell LLP on behalf of the U.S. Chamber of Commerce and the Business Roundtable.[30]

C. Disclosure Controls and Procedures

Finally, the SEC charged SolarWinds with violating Exchange Act Rule 13a-15, which requires companies to maintain a system of disclosure controls and procedures sufficient to ensure that information required to be disclosed is escalated internally to allow for timely disclosure decisions. Specifically, the SEC alleged that two cybersecurity incidents preceding the revelation of the Orion compromise, and an earlier discovery of another vulnerability, were not escalated to senior management in accordance with the company's incident response plan.

In dismissing this charge, the court observed, critically, that the SEC did not allege that SolarWinds lacked a system of disclosure controls and procedures. The SEC also did not "plead any deficiency in the construction" of SolarWinds' disclosure controls and procedures, which were set forth in the company's

incident response plan, and the SEC likewise failed to plead that the plan "frequently yielded errors."[31] Noting that "errors happen without systemic deficiencies," the court found that "[w]ithout more, the existence of two misclassified incidents is an inadequate basis on which to plead deficient disclosure controls."[32] The court noted that the SEC was separately incorrect in concluding that the incidents and vulnerability at issue should have been escalated under the incident response plan; while these were later found to be related to the compromise discovered in December 2020, none were objectively significant at the time, and the SEC's claim "has traction only with the benefit of post-[incident] hindsight."[33]

IMPLICATIONS

1. INTERNAL ACCOUNTING CONTROLS

The court's decisive rejection of the SEC's "internal accounting controls" claim under Section 13(b)(2)B) of the Exchange Act has significant implications for public companies beyond the cybersecurity context. As discussed in the *amicus* brief filed by the U.S. Chamber of Commerce and Business Roundtable in support of SolarWinds' motion to dismiss the claim, in recent years, the SEC has expanded its assertion of enforcement authority under the statute by reading the term "internal accounting controls" to include the entirety of companies' risk management and control functions, not limited to accounting controls. The SEC has brought enforcement actions under the provision based, for example, on criticisms of companies' stock buyback policies and the selection of an airline's domestic flight route. The SEC's theory in this case—that a company may be found to have violated the statute wherever any "asset" in its possession was "accessed" by an unauthorized party—would have allowed the SEC to assert a violation of the Exchange Act whenever a company experienced a cybersecurity breach, among other circumstances. Indeed, as discussed in an earlier Memorandum to Clients, within the past month the SEC charged another company with an accounting controls violation after the company was hacked.[34]

In recent SEC enforcement actions, two SEC Commissioners have repeatedly dissented on the basis that the SEC's reading of its authority under the provision has exceeded the power granted to it by Congress in the statute, but this is the first court opinion to address the SEC's interpretation of its authority. While the SEC may continue to seek to bring non-accounting-related charges under the provision, the court's opinion is likely to have a significant effect on the SEC's efforts to do so, and on companies' assessment of the SEC's ability to succeed in its claims.

2. ACTION AGAINST CISO AND FRAUD CLAIMS BASED ON SECURITY STATEMENT

The court's decision to dismiss almost all of the SEC's charges against the SolarWinds CISO should provide a measure of reassurance to public companies, the information technology industry and others concerned about the likely "chilling effect" of the charges on CISOs' willingness to internally discuss sensitive cybersecurity matters. The court observed the irony that the SEC alleged that the CISO deliberately concealed cybersecurity risks from senior management but based other claims against him on evidence that the CISO repeatedly raised concerns about specific cybersecurity risks to senior management. The

court also strongly echoed concerns that the SEC's allegations that certain, smaller cybersecurity-related matters should have been escalated by the CISO and disclosed reflected hindsight bias, as none were understood to be significant at the time.

The court's decision to permit the fraud claim against the CISO based on the company's Security Statement will come as a disappointment to many who expressed concerns about the charges against him. It is worth noting, however, that this claim is not based on an allegation that the company had to disclose any particular facts known to the CISO. The Security Statement was not included in any disclosure the company was required to make, but rather was written voluntarily by SolarWinds to encourage customers to have confidence in the security of the company and its products. The court's decision underscores the importance of companies having in place a process to review and ensure the accuracy of statements they make outside of their securities filings. In addition, while the court found that the CISO's statements in blogs and podcasts were not actionable based on their specific content, the SEC's charges underscore the importance of companies having a process in place to ensure that public statements by senior leaders in technology, such as CTOs, CIOs and CISOs, are vetted to the same degree as those made by the most senior executives of the company. Both the SEC and court emphasized the particular importance of statements about security in the information technology industry.

3. FORM 8-K FILINGS AND RISK FACTORS

The court's opinion is noteworthy in emphasizing the importance of analyzing the "overall picture" conveyed by the company's Form 8-K disclosures. While the SEC focused narrowly on several words that it alleged could create a false impression that SolarWinds was unaware of whether a compromise had occurred, the court focused on the "heart" of the disclosure, which "by any measure reported brutally bad news for SolarWinds." The court recounted the paragraphs of description in the company's Form 8-Ks of a nation-state cyber attack that had rendered up to 18,000 customers of SolarWinds vulnerable to exploitation from the time the customers began using the relevant version of the software.

The opinion is also important, and will provide some comfort to public companies, in repeatedly emphasizing that the SEC's allegations that certain facts should have been disclosed reflected hindsight bias by the agency. The court emphasized the need to review the securities filings by focusing on what was known by the company at the time of the disclosure, and not on facts that were not understood to be significant at the time. With that said, public companies should continue to consider when making public disclosures that those disclosures will be viewed with the benefit of hindsight.

The court's additional emphasis on the speed at which SolarWinds had to issue the Form 8-Ks, and how little the company knew about the incident as it was rapidly unfolding at the time, should provide some comfort to companies as they make good-faith disclosure decisions. Conversely, the fact that the SEC Enforcement Division appears to have shown little consideration for these facts is concerning given the agency's July 2023 adoption of new rules requiring disclosure of a significant amount of information about

material cybersecurity incidents on Form 8-K within four business days, as detailed in our earlier Memorandum to Clients. Determining the nature, scope, and material impact, or reasonably likely material impact, of an incident, and adequately and accurately disclosing those facts, within the SEC's prescriptive four-day deadline may be challenging for companies depending on the circumstances, as the SolarWinds case illustrates.

4. DISCLOSURE CONTROLS AND PROCEDURES

The court's dismissal of the SEC's Exchange Act Rule 13a-15 charge made clear that a disclosure controls and procedures violation requires "systemic deficiencies," not just one-off errors, particularly those apparent principally in hindsight. In explaining that the SEC failed to allege either a deficiency in the construction of SolarWinds' incident response plan or that the framework "frequently yielded errors," the opinion focused squarely on the text of the rule. The court's reasoning will be helpful to companies facing SEC criticism for discrete alleged lapses that occurred notwithstanding a reasonably designed and implemented system of disclosure procedures and controls.

* * *

ENDNOTES

1 SolarWinds Corp., Current Report (Form 8-K) (Dec. 14, 2020) ("Form 8-K"), available at https://www.sec.gov/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm ("Dec. 14 Form 8-K").

2 Press Release, White House, Background Press Call by Senior Administration Officials on Russia (Apr. 15, 2021), available at https://www.whitehouse.gov/briefing-room/press briefings/2021/04/15/background-press-call-by-senior-administration-officials-on-russia/.

3 Amended Complaint at ¶¶ 68, 73.

4 *Id.* at ¶ 157.

5 *SEC* v. *SolarWinds Corp.*, 1:23-CV-09518 (S.D.N.Y. July 18, 2024), at 53 ("Opinion").

6 *Id.* at 54.

7 *Id.* at 56.

8 *Id.* at 57.

9 *Id.* at 59.

10 *Id.* at 51.

11 Amended Complaint at ¶¶ 219-225.

12 Opinion at 67-68.

13 *Id.* at 70-71.

14 *Id.* at 72.

15 *Id.* at 81.

16 *Id.* at 72.

17 *Id.* at 73.

18 *Id.* at 78.

19 *Id.* at 76.

20 SolarWinds Corp., Current Report (Form 8-K) (Dec. 14, 2020) ("Form 8-K"), available at https://www.sec.gov/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm .

21 Opinion at 90, 88.

22 *Id.* at 90.

23 *Id.*

24 *Id.* at 86.

25 Amended Complaint at ¶ 322.

26 Opinion at 95, 100.

27 *Id.* at 100.

28 *Id.* at 98-99.

29 *Id.* at 101.

30 Brief of Amici Curiae Chamber of Commerce of the United States of America and Business Roundtable, *SEC* v. *SolarWinds Corp.*, 1:23-CV-09518 (S.D.N.Y. Feb. 2, 2024), ECF No. 68-1.

31 Opinion at 104.

ENDNOTES (CONTINUED)

32 *Id.*

33 *Id.* at 106.

34 In the Matter of R.R. Donnelley & Sons Co., Release No. 100365 (June 18, 2024), available at https://www.sec.gov/files/litigation/admin/2024/34-100365.pdf

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 900 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.