BCLP. Client Intelligent

BCLPSecCorpGov.com

SDNY DISMISSES MAJORITY OF SEC LANDMARK CHARGES AGAINST SOLARWINDS AND CISO

Jul 26, 2024

WHAT HAPPENED

On July 18, 2024, District Court Judge Engelmayer of the Southern District of New York issued his 107-page opinion and order dismissing most – but not all – of the landmark allegations of the SEC against SolarWinds Corp. and its chief information security officer.

The court found that the SEC viably alleged that the security statement (Security Statement), published by the company as its official response to customer questionnaires about its cybersecurity practices, was materially false and misleading – citing various internal presentations and communications. However, the court dismissed:

- Claims of securities fraud and false filings based on other statements and filings made prior to the notorious SUNBURST cyber-hack in late 2020.
- Claims of securities fraud and false filings based on alleged deficiencies in Form 8-Ks reporting of the SUNBURST hack as "impermissibly rely[ing] on hindsight and speculation."
- Claims of deficiencies in the company's internal accounting controls as based on an overly broad reading of the relevant statutory language.
- Claims of deficiencies in the company's disclosure controls and deficiencies as unjustified based on then apparently isolated incidents.

TAKEAWAYS

The decision provides some comfort that at least some courts will refrain from conducting rigorous hindsight examinations of good faith disclosures. Although the SEC has yet to respond (or appeal), the case provides a few lessons for public companies and senior officers:

- **Review public claims about cybersecurity; temper internal communications.** Companies and individual officers should remain vigilant about properly couching statements in presentations and other internal communications and ensuring that public statements about cybersecurity

are accurate and up-to-date – even those that may be primarily customer-focused. Although the court dismissed some self-serving declarations by the company in podcasts, press releases and blog posts as mere "corporate puffery," it sustained claims against the company and CISO that the Security Statement was misleading, based on various internal presentations and communications. Further, some believe these charges may discourage frank self-assessments and detailed reporting to senior management about cybersecurity risks and potential remedial actions in cases where cybersecurity teams feel pressure to support their companies' public assurances about the strength of their cybersecurity practices. Companies should consider developing best practices for utilizing attorney-client privilege to the extent practicable, and training teams on good hygiene in their internal communications.

- **Review specificity of risk disclosures.** The court rejected claims based on the failure to mention two recent incidents in 8-Ks and risk factors that were initially viewed as unrelated, noting that "maximum specificity" is not required. However, the court did rely on the detailed discussion in those disclosures of potential vulnerabilities and consequences of cyber-intrusions to establish their sufficiency – leaving uncertain how broadly applicable the decision should be viewed. As a result, companies should carefully evaluate risk factors for updating in periodic filings and avoid characterizing risks as purely hypothetical if they have already occurred. Further, the court also noted the company's uncertainty about the significance of the incidents during the then still ongoing investigation.

- **Stay current on 8-K cybersecurity disclosure requirements.** The alleged disclosure deficiencies pre-date the SEC's new cybersecurity disclosure rules that require 8-K reporting within four business days after the company determines an incident is material, as discussed in our July 27, 2023 post. The SEC could seek to test similar types of allegations in future cases relying on these new requirements.

- **Maintain cybersecurity controls.** The dismissal of the internal and disclosure controls claims may discourage aggressive pursuit of such theories by the SEC in the future. However, given other recent settlements, such as with R. Donnelley & Sons Co. ($2.1 million and a cease and desist order to settle disclosure and internal control failure charges relating to cybersecurity incidents and alerts), it remains unclear whether the SEC may test this theory in other forums. Accordingly, companies should continue to review and update cybersecurity controls to minimize vulnerability to future challenges.

- **Review protections for individual liability.** Although the court dismissedmost direct claims against the CISO, it sustained those related to the Security Statement based on internal presentations and communications. In that light, companies should review indemnification arrangements and insurance of cybersecurity officers.

DEEPER DIVE

As discussed in our November 1, 2023 post, the SEC charged SolarWinds and its chief information security officer (CISO) with two types of deficient disclosures:

- Misleadingly touting cybersecurity practices and products as minimally vulnerable
- Failing to disclose that the company and its customers had been victims of a large-scale cyberattack (SUNBURST), believed to have originated by Russian-sponsored hackers.

BACKGROUND LEADING UP TO DISCOVERY OF CYBER-ATTACKS

According to the SEC's complaint, as described by the court:

In January 2019, threat actors later responsible for the SUNBURST cyberattack accessed SolarWinds' corporate VPN --exploiting a cybersecurity weakness that an engineer had identified six months earlier. Through November 2020, threat actors repeatedly "conducted reconnaissance, exfiltration, and data collection; identified product and network vulnerabilities; harvested credentials of Solar Winds employees and customers; and planned additional attacks against SolarWinds' products."

By exploiting the VPN connection, the threat actors were able to "elevate privileges, disable antivirus software, and access and exfiltrate data, including computer code and customer information, without triggering alerts from SolarWinds' data loss prevention software." They used multiple accounts with administrative privileges to access and monitor emails of key personnel without detection. Between December 2019 and December 2020, they "exfiltrat[ed] approximately 7 million emails from more than 70 SolarWinds employees."

In November 2019, they used information gained from their unauthorized access to undertake a trial run of the SUNBURST attack. They first inserted non-malicious test code into the company's Orion software builds. In February 2020, seeing that the test code had gone undetected, they began inserting malicious code. Over the next several months, they inserted malicious code into three different Orion software builds used by approximately 18,000 customers, including many federal and state government agencies, and more than 1,500 publicly traded U.S. companies, banks, broker-dealers, accounting firms, and other SEC-regulated entities. The malicious code gave them a backdoor into customer networks.

In early 2020, at least nine SolarWinds customers who were MSPs suffered attacks through SolarWinds' MSP products. The threat actors used accurate credentials on their first attempt to gain access, suggesting that they had obtained customer credentials. The attacks led SolarWinds to investigate whether its database of customer credentials had been compromised but was unable to resolve the question. In March 2020, SolarWinds learned that threat actors had attacked its MSP customers using a list of 19,000 single sign-on customers. This suggested that threat actors had information to distinguish between customers who had enabled multi-factor authentication and those who only had single-factor authentication. SolarWinds again was unable to determine how

the threat actors had obtained customer credentials and identified the company's single sign-on customers. Some employees theorized that threat actors might have accessed this information through a breach of SolarWinds' systems.

In May 2020, the U.S. Department of Justice's U.S. Trustee Program (USTP) installed and evaluated SolarWinds' Orion software on a trial basis. In June 2020, USTP notified SolarWinds about malicious activity it had noticed by the Orion software after installation – that the Orion software "reached out to contact websites with an unknown purpose." By June 2020, the CISO had become aware of the attack. After investigation, SolarWinds determined that the "BusinessLayer" portion of the Orion software was causing the software "to reach out" and "attempt[] to provide information to the website about the network on which it was located." SolarWinds also uncovered "evidence that the threat actors who were attacking [USTP] had conducted reconnaissance on the Orion platform since at least mid-2019 and were mimicking SolarWinds' communication protocols to obfuscate the malicious activity." SolarWinds' internal investigation, however, failed to uncover the root cause, leaving the vulnerability unremediated.

The USTP attack was recorded internally under the company's Incident Response Plan (IRP), which classified incidents on a scale from "0" (minimal) to "3" (high), with incidents scored as "2" or higher requiring notification of the CEO and CTO. Under the IRP's criteria, an incident was scored "2" or higher when it affected multiple customers "whose impact could have an adverse effect on SolarWinds' reputation, revenue, customer, partner or the public." This "[i]ncludes a report of compromise for which other customers are susceptible." The USTP attack was scored "0"– a "minimal" incident. The CISO thus did not need to notify the CEO or the CTO about the attack.

In October 2020, a second customer, Palo Alto Networks ("PAN"), notified SolarWinds about malicious activity by the Orion software implicating the BusinessLayer. PAN reported that it had discovered this activity during an internal "red-team exercise" and that the software was reaching out to a website and downloading a malicious file.

After the call, PAN strongly encouraged SolarWinds to handle the incident as reflecting "an external attacker." SolarWinds classified the PAN incident as "0" – a minimal incident – under the IRP, notwithstanding the assessment by some employees that the incident could be related to the USTP attack. Accordingly, the PAN incident was not reported to the CEO or CTO. SolarWinds again failed to uncover the root cause of the malicious activity, preventing it from remedying the vulnerability in the Orion software, which was then being used by thousands of customers.

In December 2020, a third customer, Mandiant, notified the company of an attack against its Orion platform. Mandiant identified the platform as the likely means of the attack. Mandiant then reverse-engineered the Orion software code and identified the root cause. On December 12, 2020, Mandiant contacted SolarWinds' CEO, and reported that SolarWinds had a vulnerability in its Orion product as a result of malicious code that a threat actor had inserted. That same day, Mandiant shared the decompiled code with the CISO and others. On December 13, 2020, after reviewing the decompiled

code supplied by Mandiant, the CISO immediately linked the Mandiant attack to the earlier May 2020 attack against USTP and the October 2020 cyber-incident involving PAN.

On December 14, 2020, the company filed a Form 8-K reporting that malicious code had been inserted into the Orion platform. On December 17, 2020, SolarWinds filed a second Form 8-K with the SEC with an update on the SUNBURST attack. On January 11, 2021, SolarWinds filed a third Form 8-K, reporting additional information and findings from its investigation of the SUNBURST attack.

DISCLOSURE CLAIMS

The SEC charged the company and CISO with securities fraud and false filing claims alleging material omissions and misstatements in the following disclosures:

- The Security Statement
- Various public statements in podcasts, press releases and blog posts
- Cybersecurity risk disclosure contained in the 2018 IPO registration statement and incorporated into later SEC filings
- The December 14 and 17, 2020 Form 8-Ks when it first disclosed the SUNBURST attack.

Sustaining of claims of Security Statement as misleading. The court sustained the SEC's securities fraud claims on the basis that the Security Statement made material misrepresentations as to the state of the company's cybersecurity. The company published the Security Statement as its official response to customer questionnaires about its practices. Among other statements, the Statement represented that the company:

- Complied with the National Institute of Standards and Technology (NIST) Cybersecurity Framework for evaluating cybersecurity practices.
- Used a secure developmental lifecycle to create its software products.
- Employed network monitoring.
- Had strong password protections
- Maintained good access controls.

The SEC viably alleged that, in each of these five areas, the company was chronically deficient – as documented in internal assessments, presentations and communications that showed that employees recognized systemic cybersecurity deficiencies. The court found:

> "In essence, the Statement held out SolarWinds as having sophisticated cybersecurity controls in place and as heeding industry best practices. In reality, based on the pleadings, the company fell way short of even basic requirements of corporate cyber health. Its passwords-including for key products-were demonstrably weak and the company gave far too many employees unfettered administrative access and privileges, leaving the door wide open to hackers and threat actors."

Additionally:

> "The [SEC's complaint] thus amply pleads, with particularity, that [the CISO] knew of the substantial body of data that impeached the Security Statement's content as false and misleading. His conduct in allowing the Statement to issue publicly, and to remain in place for years, in the face of company practices inconsistent with it, is plausibly pied as "highly unreasonable or extreme misconduct." . . . [His] scienter is also properly imputed to SolarWinds."

Dismissal of claims based on finding of press releases, blog posts as mere "puffery". The court dismissed claims based on other public statements touting the company's cybersecurity practices as non-actionable corporate puffery, "too general to cause a reasonable investor to rely upon them." The court found 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."

Dismissal of claims based on finding of cybersecurity risk disclosure as sufficient. The court dismissed claims based on risk disclosures included in the 2018 IPO registration statement and incorporated in subsequent filings, finding that they adequately addressed unique risks the company faced. The court concluded:

- Case law does not require companies to spell out in substantially more specific terms scenarios under which its cybersecurity measures could prove inadequate.
- Anti-fraud laws do not require cautions to be articulated with maximum specificity.
- As a policy matter, "maximal specificity 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."

The court also rejected the SEC's view that the risk disclosure became misleading because the company failed to update it to account for the USTP and PAN incidents. In the court's view, the risk disclosure already sufficiently warned investors of the vulnerability of the company's systems to cyberattacks and that it could not anticipate or prevent all such intrusions:

> "In light of this fulsome disclosure, Solar Winds did not have a duty to disclose the fact of individual cyber intrusions or attacks. It had already disclosed the likelihood of these as, regrettably, a fact of life."

The court acknowledged that, with hindsight, the incidents could be seen as prefiguring SUNBURST, but found that the SEC did not plausibly plead that, before SUNBURST, the company had concluded it had been victim to a material systemic intrusion. On the facts as pled, the company was unable to determine the "root cause" of either intrusion.

> "An updated disclosure could say little more than that the company was investigating but had not reached a conclusion as to two customer-reported incidents involving Orion. The SEC has not cited authority supporting a legal duty to update its risk disclosure in the face of this level of knowledge. . . . [G]iven the uncertain character, source, and relatedness of the two incidents, SolarWinds had not determined that the material risks of which it had warned had in fact transpired."

Dismissal of claims based on finding of 8-K disclosures as sufficient. The court dismissed the SEC's securities fraud and false filing claims based on SolarWinds' December 14 and 17, 2020 Form 8-Ks, in which it disclosed the SUNBURST attack but did not disclose the USTP and PAN incidents. In the court's view:

- The 8-Ks sufficiently disclosed information at those early stages of its investigation, when its understanding of the attacks was still evolving.
- The omission of the two incidents could be actionable only if disclosure was necessary to make the Form 8-K not
- The heart of the Form 8-K's disclosure – that a cyberattack had "inserted a vulnerability within [SolarWinds'] Orion monitoring products" and that the vulnerability "if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run" -- fairly captured the known facts and was faithful to what SolarWinds then knew from its customers.

INTERNAL ACCOUNTING CONTROLS CLAIMS DISMISSED

The court dismissed claims of deficiencies in internal accounting controls as based on an overly broad reading of the relevant statutory language. The SEC had alleged that the company's source code, databases and products were vital asssets and that the company failed to protect them due to poor access controls, weak internal password policies and VPN security gaps. The court found that the relevant statute only covers internal accounting controls – not cybersecurity controls – and that construing the statute more broadly would have "sweeping ramifications," stating:

> "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. That construction –and those outcomes –– cannot be squared with the statutory text."

In the court's view, the statute was designed to assure books and records accurately and fairly reflected transactions and the disposition of assets, to protect the integrity of the independent audit, and to promote reliability and completeness of financial information that is disseminated to investors. In particular, Congress's explicit purpose was to provide reasonable assurances that, among other things, transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted *accounting principles* or any other applicable criteria.

DISCLOSURE CONTROLS CLAIMS DISMISSED

The court dismissed claims of deficiencies in the company's disclosure controls and procedures as unjustified based on isolated incidents. The SEC had alleged that the company had ineffective disclosure controls based primarily on allegedly misclassifying certain incidents under its incident response plan (IRP) as non-serious and, as a result, failing to trigger notification to the CEO and CFO. The court dismissed the allegations, finding:

- No deficiency in the IRP itself was identified.
- Without more, the existence of two misclassified incidents is insufficient to plead deficient disclosure controls.
- The SEC cannot claim a misapplication of the IRP's standards. At the time, based on available information, the company had not uncovered the root cause or determined that the incidents were related.
- The CISO's failure to elevate the VPN vulnerability prior to SUNBURST does not evidence a failure of disclosure controls, because that was then a subject of debate.

RELATED PRACTICE AREAS

- Securities & Corporate Governance
- Data Privacy & Security

MEET THE TEAM

R. Randall Wang

St. Louis

randy.wang@bclplaw.com
+1 314 259 2149

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144
