JENNER & BLOCK

Client Alert: The SEC Charges SolarWinds and Its CISO with Fraud: Key Takeaways

Publications

November 2, 2023
By: Shoba Pillay, Charles D. Riely

This week, the SEC filed a high-profile litigation asserting fraud and internal controls charges against software company SolarWinds Corporation and its Chief Information Security Officer, Timothy G. Brown, in connection with a massive 2020 breach of SolarWinds' network monitoring software system, Orion.[1] The charges against SolarWinds and Brown were long-anticipated following SolarWinds' announcements in October 2022 and June 2023 that the company, its CFO, and CISO had received Wells Notices from the SEC indicating an intention to charge each of them.[2]

In 2023, the SEC brought fraud charges against SolarWinds and its CISO in connection with the Orion compromise, and we have covered the developments in this litigation here and here. In relevant part, the SEC alleged that SolarWinds, which provides various information technology management services to customers, overstated the steps it took to prevent cybersecurity incidents and then failed to tell the whole truth after it learned of a massive breach of Orion that impacted many of its key customers. According to public reporting, the SolarWinds' customers impacted by the breach included government agencies such as the Departments of Defense and State and a wide range of private companies.

The action against the company and the CISO is the SEC's most aggressive use of its powers to address a company's alleged misrepresentations related to cybersecurity risks or incidents. In fact, this is the *first* time the SEC has sued a company for *scienter*-based fraud involving cybersecurity failures; the *first* time the SEC has sued a CISO (or any individual) for their role in cybersecurity failures; and the *first* time the SEC has sued a company for internal controls failures arising from alleged cybersecurity deficiencies that led to a company's inability to protect its key assets. This article discusses the unique facts that led to this action and the key takeaways for companies and officers grappling with cybersecurity going forward.

Background

The SEC's Complaint alleges that SolarWinds and Brown misled the company's investors and customers by overstating the company's level of cybersecurity practices and concealing mounting cybersecurity risks between October 2018 and January 2021. Per the Complaint, Brown was

responsible for creating and approving a misleading "Security Statement" posted to SolarWinds' website. The Security Statement claimed that SolarWinds followed the internationally recognized National Institute of Standards and Technology Cybersecurity Framework ("NIST Framework"), that the company's development lifecycle for software creation was secure, and that its password policies and access controls were strong. Brown also signed sub-certifications attesting to the strength of the company's internal controls. In addition, Brown allegedly touted the strength of SolarWinds' cybersecurity practices in a podcast, blog post, interview, and company-approved press releases, claiming in one blog post that SolarWinds "places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards."[4]

The SEC's case against Brown centers on allegations that he was aware of critical cybersecurity deficiencies even as the company's public statements and SEC filings—including statements and filings Brown helped create and approve—concealed those deficiencies and mischaracterized the strength of SolarWinds' cybersecurity practices. These deficiencies included SolarWinds' failure to maintain a secure development lifecycle for the creation of its software products, its failure to enforce the use of strong passwords on its systems, and its failure to remedy persistent access control problems. For instance, according to the Complaint:

- In October 2018, the same month SolarWinds filed a registration statement "with only generic and hypothetical cybersecurity risk disclosures," Brown wrote in an internal presentation that the company's "current state of security leaves us in a very vulnerable state for our critical assets."

- In July 2020, Brown wrote in an email to a member of the company's engineering team, "As you guys know our backends are not that resilient and we should definitely make them better."

- In December 2020, Brown and other executives drafted and filed a Form 8-K with the SEC disclosing that threat actors had exploited vulnerabilities in Orion to insert malicious code into the software. Per the complaint, the executives did not disclose that threat actors had already exploited these vulnerabilities against SolarWinds' customers multiple times, despite the executives' awareness of these incidents. The complaint alleges that although the vulnerabilities were ones that "SolarWinds and Brown had known about for months and that could have been remedied through straightforward steps," SolarWinds and Brown failed to take such steps.

As part of its fraud case, the complaint focuses on Brown's alleged exercise of options and sale of options for more than $170,000 as the profit motive for engaging in fraud during the relevant period.

The SEC's complaint also alleges that SolarWinds' cybersecurity vulnerabilities ultimately culminated in a massive cyber attack that compromised SolarWinds' "crown jewel" software platform, Orion. In the "SUNBURST" attack, hackers gained access to the networks, systems, and data of thousands of Orion's customers by inserting malicious code into the Orion product. SolarWinds learned of the

SUNBURST attack in December 2020, when a cybersecurity firm customer of SolarWinds discovered an attack against its Orion platform and notified SolarWinds.

The SEC's complaint further asserts that as an Exchange Act Section 13(a) reporting company, SolarWinds was obligated 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." In bringing this charge in the cybersecurity context, the complaint stresses that the company's internal accounting controls did not sufficiently protect its most critical assets—*i.e.*, its software code and technology infrastructure—and did not follow its own certification control concerning cybersecurity, including by failing to use and document a list of controls per Brown's certifications.

Key Takeaways

- **The SEC is taking a more aggressive stance toward cybersecurity enforcement.** The SEC's action is a sharp departure from prior actions that charged companies for failures in their policies and procedures around escalating information about data breaches. The SolarWinds Complaint involves *scienter*-based fraud charges against both a company and an individual, who allegedly profited by exercising and selling options worth a relatively low amount (approximately $170,000).

- **Companies should assess their cybersecurity statements (both internal and external) regarding the products, services, and software that are core to their business.** The SEC's Complaint focuses on SolarWinds' own statements referring to its Orion software as its "crown jewel," meaning an asset that, if compromised, could have a material impact on SolarWinds. This action signals that the SEC will likely continue to scrutinize companies' representations about their priorities to determine if their practices align with those representations.

- **The SEC's inclusion of charges that SolarWinds failed to employ internal accounting controls is also significant.** Here, unlike prior actions, the SEC charged SolarWinds not only with failing to maintain internal disclosure controls and procedures, but also with a failure to employ a system of internal accounting controls designed to provide reasonable assurance that access to the Company's assets was only in accordance with management direction. That is, the charges alleged that SolarWinds had deficient cybersecurity controls to safeguard its critical assets during a breach.

- **CISOs should understand their disclosure and controls obligations and their exposure with respect to cybersecurity.** No public statements are too informal for the SEC to consider in an investigation into potential fraud. The SEC's allegations focus on Brown's authorship of the "Security Statement" posted on the company's website and point to various public blog posts and interviews, including Brown's statement in an interview that "[m]y broad-based mission is to basically eliminate anything that is material damage to my company." The allegations also

emphasize that Brown signed sub-certifications attesting to the strength of the company's internal controls, which the SEC later deemed to be false in light of the various known cybersecurity vulnerabilities.

- **Information security personnel must be aware that their emails and other internal communications will likely be subject to scrutiny in the wake of a breach.** In fraud and internal controls enforcement actions, the SEC will likely continue to parse both the internal communications of individuals it charges and the communications of other personnel. To convey the breadth of the security vulnerabilities SolarWinds faced, the SEC's Complaint cites numerous statements made within the company by employees other than Brown, including an engineer's 2020 statement that "[w]e filed more vulnerabilities than we fixed. And by fixed, it often means just a temporary fix . . . but the problem is still there and it's huge."

Conclusion

The SolarWinds action sends the message that both companies and CISOs need to be cautious in how they describe their cybersecurity practices in light of an evolving threat landscape. Companies should consult with counsel who are familiar with both cyber risk management and SEC enforcement to ensure that they are prepared for and able to respond appropriately to cyber incidents.

Footnotes

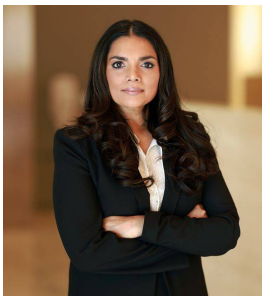
[1] *See SEC v. SolarWinds and Brown*, No. 1:23-cv-09518 (S.D.N.Y. Oct. 30, 2023), https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf.

[2] *See* SolarWinds Corp., Form 8-K (Oct. 28, 2022), https://www.sec.gov/Archives/edgar/data/1739942/000173994222000091/swi-20221028.htm; SolarWinds Corp., Form 8-K (June 23, 2023), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001739942/000173994223000079/swi-20230623.htm. The SEC has not yet announced charges against SolarWinds' then-CFO, and it is possible that more charges related to the SolarWinds attack are forthcoming.

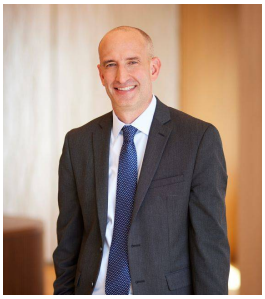
[3] Isabella Jibilian and Katie Canales, *What Is the SolarWinds Hack and Why Is It a Big Deal?*, Business Insider (Apr. 15, 2021), https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[4] Complaint ¶ 115, *SEC v. SolarWinds and Brown*, No. 1:23-cv-09518 (S.D.N.Y. Oct. 30, 2023), https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf.

Related Attorneys



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605



Charles D. Riely
Partner
criely@jenner.com
+1 212 891 1686

Related Capabilities

Data Privacy and Cybersecurity

Investigations, Compliance, and Defense

Stay Informed →