ALSTON & BIRD

WWW.ALSTON.COM

Securities Law / Securities Litigation / Privacy, Cyber & Data Strategy
ADVISORY ■

NOVEMBER 10, 2023

The SEC Sues SolarWinds and Its CISO for Alleged Fraud and Disclosure Controls Failures

by Cara Peterman, Kim Peretti, Dave Brown, Kate Hanniford, Sierra Shear, *and* Madeleine Juszynski

In the latest development in a nearly three-year saga since SolarWinds Corporation announced that it had learned of a "highly sophisticated, manual supply chain attack" on its systems, the SEC filed a civil complaint against SolarWinds and its current Chief Information Security Officer (CISO) and former head of Information Security, Timothy Brown, alleging claims for fraud and disclosure control violations. Notably, the filing of the complaint represents the first formal action by the SEC against a CISO in this context and the first time the SEC has gone to court with civil fraud claims against a public company related to their cybersecurity disclosures. The action provides yet another indication of the agency's increased focus on cybersecurity disclosures, on the heels of the SEC's new cybersecurity disclosure rules for public companies, adopted earlier this year.

The SEC's Complaint

In December 2020, SolarWinds disclosed that it had learned of a cybersecurity attack (referred to as the SUNBURST attack) impacting its Orion Platform, one of the company's "crown jewel" assets that was used by numerous public and private sector organizations for IT infrastructure monitoring and management. In November 2022, SolarWinds announced that the company had received a Wells Notice indicating that SEC staff had made a preliminary determination to recommend that the SEC file an enforcement action against the company for securities laws violations with respect to its cybersecurity disclosures and public statements, as well as its internal controls and disclosure controls and procedures. In June 2023, the company announced that its CFO and Brown had also received Wells Notices. On October 30, 2023, the SEC filed suit against SolarWinds and Brown in the Southern District of New York.

The SEC's complaint alleges that Brown made or approved a number of purported misstatements about the state of the company's cybersecurity program, including statements on the company's website, in blog posts, and in podcasts. The complaint additionally alleges that the company's SEC filings contained false and misleading statements about the company's cyber risks, and that the company's disclosure of the SUNBURST attack omitted material information. In support of its allegations, the SEC cites to, among other

things, internal emails and messages among members of the company's cybersecurity team. The evidence cited by the SEC shows a particular focus on the issues that were allegedly raised to Brown and his response.

Allegations regarding statements on the company's website, in blogs, and in press releases

The SEC alleges that the company and Brown made numerous false statements to investors about the strength of the company's cybersecurity practices and the security of its products. These statements allegedly misled investors who – the SEC contends – would consider the true state of the company's cybersecurity practices and vulnerability to a cyberattack as "significant" in making their investment decisions.

First, the complaint repeatedly references a "Security Statement" posted to the company's website that stated in part that the company: (1) followed certain standardized industry best practices used for creating software products with robust cybersecurity protections (the "Secure Development Lifestyle" (SDL) protections); (2) enforced the use of complex passwords on all information systems and databases; (3) granted access to sensitive data on a "need-to-know / least privilege necessary" basis; (4) limited the number of company employees able to deactivate anti-virus software or change user passwords; and (5) followed the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Internal documents identify Brown as the ultimate "owner" or "approver" of the Security Statement.

The SEC alleges, however, that the Security Statement concealed the company's purportedly poor cybersecurity practices from the public, including the company's alleged failure: (1) to routinely measure or enforce compliance with the SDL protections; (2) to enforce the use of strong passwords on all systems; and (3) to remedy long-standing access control issues.

The complaint next alleges that the company, and Brown specifically, made numerous public statements about the strength of SolarWinds' cybersecurity program in various press releases, blog posts, and podcasts, including that the company "places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards." The complaint alleges that these and similar statements were false and misleading, based on internal emails, messages, and documents from 2017 to 2020 that purportedly show that company employees and executives, including Brown, were aware of the company's allegedly poor cybersecurity practices and critical vulnerabilities as early as 2018. The evidence cited by the SEC includes:

- January 2018 emails acknowledging that the company was not following the practices outlined in the Security Statement's SDL section as published on the company website, and that the company would begin incorporating those practices in 2018; a subsequent August 2019 presentation that listed the SDL practices as an area where the company did "not routinely measure or enforce policy compliance"; and sworn testimony from Brown that Orion was not built under an SDL in 2020.
- A June 2018 email from a company network engineer that warned that the company's remote access VPN allowed access from devices not managed by the company and explaining that a threat actor who found that vulnerability could "basically do whatever without us detecting it until it's too late," which would lead to a "major reputation and financial loss" for the company.
- Documents demonstrating known vulnerabilities in the Orion Platform, including a September 2020 internal "Risk Acceptance Form" warning of "the risk of legacy issues in the Orion Platform" and that "[t]he volume of security issues being identified over the last month have outstripped the capacity of

Engineering teams to resolve"; and November 2020 instant messages to a senior information security manager containing a list of vulnerabilities in the Orion Platform and stating that "the products are riddled and obviously have been for many years."

- An October 2020 message from an information security employee stating that he "lied" when a customer asked the company if it had seen similar activity to cyberattacks on the customer and the company employee denied seeing similar activity.
- A November 2020 instant message from a senior information security manager stating that "[w]e're so far from being a security minded company. [E]very time I hear about our head geeks talking about security I want to throw up."

The SEC alleges that this evidence rendered Brown and the company's statements about the state of its cybersecurity program false and misleading.

Risk disclosures in periodic SEC filings

The SEC additionally alleges that the "generic and hypothetical" cybersecurity risk disclosure in the company's registration statements filed in connection with its 2018 IPO failed to disclose cybersecurity risks that were known to the company and Brown at the time of the filing and that those allegedly misleading risk disclosures were repeated verbatim in the company's periodic SEC filings between October 2018 and November 2020. The SEC claims that these "generic" disclosures about the company's hypothetical cybersecurity risks were false and misleading because they failed to disclose known risks about the scale of cybersecurity risk to the company and the company's failure to follow the practices outlines in the Security Statement.

Statements about the SUNBURST incident in SolarWinds' December 14, 2020 Form 8-K

Finally, the complaint contests the accuracy of the company's statement in its December 14, 2020 Form 8-K that it had "been made aware of a cyberattack that inserted a vulnerability within its Orion monitoring products which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run," and that the company was still investigating the attack. The SEC alleges that the Form 8-K contained false and misleading statements that led investors to believe that the company was still investigating whether threat actors had access to company servers, when the company definitively knew at the time of the filing that threat actors had compromised company servers on at least three occasions since May 2020.

In support of its claims, the SEC cites Brown's testimony that, upon learning of a cyberattack on a company customer on December 12, 2020, no further work was necessary for him to link it to the three cybersecurity attacks that the company had previously uncovered between May and December 2020. The SEC also alleges that Brown signed sub-certifications falsely confirming that all material cyber incidents had been disclosed to the company's executives responsible for its filings, despite his awareness of the prior cyber incidents.

Allegations related to disclosure controls

The complaint also alleges the company maintained deficient disclosure controls, which failed to ensure that information about potentially material cybersecurity risks and concerns were reported to executives responsible for disclosures. For instance, the SEC alleges that the company's Incident Response Plan required a report to management responsible for disclosure only for those incidents that simultaneously impacted

multiple customers. The SEC alleges that "as a result, multiple cybersecurity issues that had the potential to materially impact SolarWinds, but which SolarWinds determined at the time did not yet impact multiple customers, went unreported."

Takeaways

Public companies, their officers and directors, and their in-house counsel should consider taking proactive steps in light of this first-of-its-kind action by the SEC, including:

- Executives should recognize that this case signals an increased focus by the SEC on CISOs and expanding potential liability for corporate officers beyond the CEO and CFO. The SEC is likely to continue to focus on enforcement actions in this arena, in particular in light of the agency's recently implemented cybersecurity disclosure rules for public companies.
- Information security management should work closely with counsel to confirm the accuracy of the company's public filings regarding its cybersecurity risks, controls, and procedures, even if the company's statements may be akin to "puffery." This is especially true when drafting the upcoming 10-K disclosures.
- Employees should understand that the SEC may point to inflammatory language within employee communications as support for their claims and should exercise caution when discussing the state of the company's cybersecurity program and response to any cybersecurity incident, including by email, chat, and text message.
- CISOs and other senior information security management should recognize that liability under the federal securities laws is not limited to statements made in formal SEC filings and that their public statements – including documents posted to the company website, blog posts, and presentations at conferences – may be scrutinized by the SEC and shareholder plaintiffs if there is a significant cybersecurity incident. These statements should be analyzed in conjunction with the company's 10-K disclosures.
- Public companies and their directors and officers should evaluate their cybersecurity and D&O insurance policies to assess coverage for investigations and claims involving CISOs and other cybersecurity officers and employees.
- Employees working to respond to an incident or analyze the state of a company's cybersecurity program should consider when to include counsel in ongoing discussions to ensure that the company's disclosures reflect the most up-to-date information.

You can subscribe to future advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you would like more information, please feel free to contact one of the attorneys in our **Securities Group**, **Securities Litigation Group**, **Privacy, Cyber & Data Strategy Group**

.

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: Vantage South End ■ 1120 South Tryon Street ■ Suite 300 ■ Charlotte, North Carolina, USA 28203-6818 ■ +1 704 444 1000 ■ Fax: +1 704 444 1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: City Center Fort Worth ■ Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ +1 214 922 3400 ■ Fax: +1 214 922 3899
LONDON: LDN:W ■ 6th Floor ■ 3 Noble Street ■ London ■ EC2V 7DE ■ +44 20 8161 4000
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 755 Page Mill Road ■ Building C - Suite 200 ■ Palo Alto, California, USA 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333