The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 35502

November 2, 2023

SEC Charges SolarWinds Corp. and its CISO for Fraud Based on their Misrepresentations Regarding the Firm's Cybersecurity

[35502]

November 02, 2023

TO: ICI Members
Chief Compliance Officer Committee
Chief Information Security Officer Committee
Operations Committee
SEC Rules Committee
Technology Committee SUBJECTS: Cybersecurity
Litigation & Enforcement
Technology & Business Continuity RE: SEC Charges SolarWinds Corp. and its CISO for Fraud Based on their Misrepresentations Regarding the Firm's Cybersecurity

On October 30, 2023, the Securities and Exchange Commission filed a complaint against SolarWinds Corporation and its Chief Information Security Officer (CISO), Timothy G. Brown, alleging various violations of the Securities Act of 1933 and the Securities Exchange Act of 1934, including the antifraud provisions in both acts.[1] The SEC's Complaint seeks a jury trial in the case and penalties including permanent injunctions against the defendants, disgorgement of ill-gotten gains, and payment of a civil monetary penalty. In addition, the Commission seeks an order permanently prohibiting the CISO from acting as an officer or director of any issuer of publicly-registered securities. The Commission's allegations in support of these sanctions are summarized below.

The Defendants: SolarWinds and Brown

According to the Compliant,[2] SolarWinds is a public company that "designs and sells network monitoring software used by many businesses, as well as state, federal, and foreign governments to manage their computer systems." The firm's products "provide information technology professionals with visibility into network utilization and equip information technology departments to detect, diagnose, and resolve network performance issues." During the period covered by the SEC's Complaint (i.e., October 2018 through at least January 12, 2021),[3] SolarWinds had more than 300,000 customers, including 499 of

the Fortune 500 companies.

Defendant Timothy G. Brown served as SolarWinds' Vice-President of Security and Architecture and, in January 2021, he became the firm's Chief Information Security Officer (CISO). As the person responsible for the firm's overall security program, he was the firm's primary cybersecurity spokesperson and, in that role, he made numerous public disclosures regarding the state of SolarWinds' cybersecurity practices. These disclosures included: the firm's "Security Statement," that was posted to SolarWinds' website; SEC filings (Forms S-1 and S-8 Registration statements); periodic reports including the firm's Form 8-Ks; podcasts; blog posts; and press releases. He also signed sub-certifications attesting to the adequacy of the firm's cybersecurity internal controls, which SolarWinds' executives relied on in connection with making SEC filings.

The Alleged Violations of the Federal Securities Laws

The Compliant includes the following ten claims for relief:

- First Claim: SolarWinds and Brown committed fraud under Section 17(a) of the Securities Act of 1933;
- Second Claim: Brown aided and abetted SolarWinds' violations of Section 17(a);
- Third Claim: SolarWinds and Brown committed fraud under Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5(b) under the Act;
- Fourth Claim: Brown aided and abetted SolarWinds' violations under the '34 Act;
- Fifth Claim: SolarWinds violated Section 13(a) of the '34 Act and rules thereunder. These provisions require issuers of securities registered with the SEC to file with the SEC factually accurate annual reports (on Form 10-K), quarterly reports (on Form 10-Q), and current reports (on Form 8-K). In addition to the required information in these reports, the SEC's rules require issuers to add such further material information that is necessary to make the reported information not misleading;
- Sixth Claim: Brown aided and abetted SolarWinds' reporting violations under the '34 Act;
- Seventh Claim: Violations of Section 13(b)(2)(B) of the '34 Act for failing to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that SolarWinds' access to assets is permitted only in accordance with management's general or specific authorization;
- Eighth Claim: Brown aided and abetted SolarWinds' violations of Section 13(b)(2)(B);
- Ninth Claim: SolarWinds violated SEC Rule 13a-15(a) under the '34 Act by failing to maintain disclosure controls and procedures that are designed to ensure that information reported to the SEC is recorded, processed, summarized, and reported in a timely fashion; and
- Tenth Claim: Brown aided and abetted SolarWinds' violations of Rule 13a-15(a).

The factual basis behind each of these claims and the SEC's allegations supporting them are summarized below.

The SEC's Facts and Allegations

Pages 1-8 of the Complaint summarize the SEC's Complaint and the basis for its action against the Defendants. Pages 13-61 provide the details of the SEC's allegations and discuss the documents and evidence in support of the allegations. Much of this evidence came from the Defendants' records, such as internal communications (emails and texts) and presentations that were contrary to the public statements the Defendants made about the adequacy of SolarWinds' cybersecurity. As discussed in detail in the Complaint:

The Defendants Falsely Promoted SolarWinds' Cybersecurity Practices in Public Statements

The Complaint evidences that, throughout the relevant period, the Defendants made false public statements touting the quality of SolarWinds' cybersecurity practices. They also posted – prior to an initial public offering (IPO) of the company's shares – a "Security Statement" on its public website. This Statement, which Brown was primarily responsible for creating and approving prior to its posting, purported to describe SolarWinds' cybersecurity practices. The Statement was also used to respond to inquiries from the public and customers about the company's cybersecurity practices.

The Statement "contained multiple materially false and misleading statements, assuring the public that SolarWinds followed well-recognized cybersecurity practices when, in reality, [its] cybersecurity practices fell significantly short of those practices." The misrepresentations in the Statement includes statements regarding the company's compliance with the NIST framework; its use of a secure development lifecycle when creating software for customers; its use of strong password protections; and its maintenance of good access controls. (Complaint at ¶ 45.)

The Defendants Misleadingly Claimed to Follow the NIST Framework for Evaluating Cybersecurity Practices

SolarWinds' Security Statement claimed that it followed the NIST Cybersecurity Framework including by having layered security controls to help identify, prevent, detect, and respond to security incidents. Despite these claims, SolarWinds met only a small fraction of the cybersecurity controls in the NIST Framework, and it had no program or practice in place for the majority of the NIST controls, as next discussed.

SolarWinds Had No Policy or Practice in Place for Most of the NIST Framework

A 2019 assessment of SolarWinds' adherence to the NIST Framework found that it had a program or practice in place for only 198 of the 325 NIST controls (6%) and no program or practice in place of 198 of the 325 controls (61%). The company's 2021 assessment found that only 40% of the NIST controls were met or partially met, leaving 60% [of the NIST controls] "completely unmet." (Complaint at ¶¶ 50-51; emphasis in original.)

The Defendants Falsely Claimed that the Company Followed a Secure Development Lifecycle when Creating Software for Customers

While the company's Security Statement claimed that it followed a defined Secure Development Lifecycle (SDL) to develop software designed to increase the resiliency and security of its products, this was not the case. According to the Complaint, the company failed to follow an SDL, including for components of its "crown jewel," which was the Orion platform. [This was the platform that was used in the SUNBURST attack discussed below.] An internal email from SolarWinds' Chief Information Officer (CIO) to senior managers "bluntly admitted that the Security Statement's SLD section was false. Rather than suggest amending [the Statement] to make it accurate . . . SolarWinds would continue to hide the falsity of these statements and work towards making them eventually true . . .." According to the Complaint, this conduct, rather than reflecting a culture of honesty or effective controls, instead "reflects a culture of recklessness, negligence, and scienter" and it "is also evidence of a scheme to conceal the true state of SolarWinds' cybersecurity practices from both its investors and customers." (Complaint at ¶¶ 62-63.)

The Defendants Falsely Claimed that SolarWinds Implemented a Strong Password Policy

SolarWinds' password policy, which was incorporated by reference into their Security Statement, required passwords to: (1) be changed every 90 days; (2) have a minimum length of eight characters; and (3) include three of the following four specified characteristics (i.e., upper case letter, lower case letter, a number between 0-9, and a non-alphanumeric character). Notwithstanding this policy, SolarWinds did not enforce strong passwords for users of all of its information systems, applications, and databases. While there were "multiple instances" of password problems flagged within SolarWinds, they were not acted upon. These instances included: default passwords in SolarWinds products were still being used, including the default password "password"; shared legacy account login credentials that were being used even though SolarWinds required authorized users to use unique account IDs; database passwords that were not encrypted within the configuration file; login credentials that were stored in plain text in configuration files; and passwords that were stored in plain text on the public web server in the web configuration file and in the system registry of the machine. Passwords were not individually stored in an encrypted state as stated in the company's Security Statement.

A September 2019 internal email noted the use of passwords that were not compliant with the company's policy. This is because passwords did not need to comply with the company's password protocols, passwords could be reused, and passwords were not required to be changed at a set number of days. In addition to these concerns, the Complaint notes that, in November 2019, an outside security researcher notified SolarWinds that the password for the company's Akamai server, which was used to distribute software to clients, was publicly available and could be used by a threat actor to infect SolarWinds software updates. (Complaint at ¶¶ 78-83.)

The Defendants Falsely Claimed that the Company Maintained Strong Access Controls

SolarWinds Security Statement noted that it: used role-based access controls; employees were only granted access to information resources based on their specific job function; and the firm took a "least privilege necessary" approach to access. As described in the Complaint, however, SolarWinds' "access control environment was diametrically different" from that described in the Security Statement and "SolarWinds actually had poor access controls - a problem that it failed to remedy for years." In support of this conclusion, the Complaint notes that, between, 2017 and 2020, SolarWinds "routinely and pervasively granted employees unnecessary 'admin' rights, giving them access and privilege to more systems than necessary for their work functions" and "there is evidence that most employees had 'Admin' rights" during the relevant period. (Complaint at ¶¶ 91-92.)

As further support for this claim, the Complaint cites an August 2019 Security & Compliance Program Quarterly Review that Defendant Brown prepared that acknowledged that "Access and privilege to critical systems/data is inappropriate." It also noted that SolarWinds had a NIST score of 1, meaning that it had an ad-hoc, inconsistent, and reactive approach to meeting NIST's Authentication, Authorization, and Identity Management controls. SolarWinds' access controls also did not satisfy the Fed RAMP security control requirements: of the 43 controls because only two were "in place." Eighteen were listed as "may be in place," and 23 were rated "No program/practice in place." (Complaint at ¶¶ 97-98.)

In addition to the above access control concerns, in 2018, a SolarWinds engineer identified

a security gap relating to the company's VPN. In particular, "a user with credentials could evade SolarWinds' data loss prevention software by logging on to SolarWinds' VPN network from a device that was not owned or managed by the company's IT Department. This vulnerability was exacerbated by the fact that many SolarWinds' employees had administrator rights that would enable them to make changes to security settings. These VPN vulnerabilities were highlighted by the SolarWinds engineer in an August 2018 presentation. His presentation noted that SolarWinds' set up was "not very secure" and "someone exploiting the vulnerability 'can basically do whatever without us detecting it until it's too late' which could 'lead to 'major reputation and financial loss' for SolarWinds." Notwithstanding the engineer's concerns, the Complaint notes that SolarWinds and Brown "took no steps to remediate the vulnerability in 2018 or 2019." SolarWinds' 2018 IPO offering failed to include any mention of these vulnerabilities. This omission deprived investors of key information about the company. (Complaint at ¶¶ 102-110.)

Brown Made Misrepresentations in Company-Approved Press Releases, Blog Posts, and Podcasts

The Complaint cites various public comments made by the Defendants touting their "heavy-duty" cyber hygiene; their focus on "things that . . . make up cyber best practices; and that the company "places a premium on the security of its products and makes sure everything is backed up by sound security processes, procedures, and standards." (Complaint at ¶¶ 113-117.)

SolarWinds Had Pervasive Cybersecurity Deficiencies

In support of this claim, the Complaint incorporates the issues discussed above. It also discusses internal communications that include the following statements:

- SolarWinds needs to "lock down [its] critical assets that could cause a major event" and that the "[c]urrent state of security leaves us in a very vulnerable state for our critical assets."
- Problems with SolarWinds' security initiative included that there was "No true expertise for security" and that "core SolarWinds teams do NOT understand security" and
- "[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."

(Complaint at ¶¶ 120-123.)

SolarWinds Made Materially False and Misleading Statements About its Cybersecurity Practices in its SEC Filings

The Complaint quotes from SolarWinds' October 2018 Form S-1, which the company filed as a publicly-traded company, and notes that its disclosure "recited the harm that could befall SolarWinds and generic and hypothetical cybersecurity risks that most companies fact. But it did nothing to alert investors to the elevated risks that existed at SolarWinds." At the time of filing this disclosure, Brown stated internally that the "current state of security leaves us in a very vulnerable state for our critical assets." The Complaint notes that, despite its known cybersecurity issues and their severity, "SolarWinds neither specifically disclosed the issues nor generally disclosed that known, unremediated issues with NIST compliance, SDL, access controls (including the known VPN vulnerability), or passwords, existed. Nor did SolarWinds even disclose Brown's assessment that it was 'very vulnerable' to a cyberattack." These misleading risk disclosures were repeated in at least thirteen SEC filings (i.e., in their 10-Q, 10-K, S-8, and S-1 filings) made between November 27, 2018 and

November 5, 2020. (Complaint at ¶¶ 130--138.)

SolarWinds and Brown Failed to Disclose Red Flags and Warning Signs of a Cyberattack Leading up to the Revelations of the SUNBURST Cyberattack

The Complaint notes that, as a result of SolarWinds' failure to remediate the above-described issues, "threat actors were able to later exploit the still unremediated VPN vulnerability to access SolarWinds' internal systems in January 2019, avoid detection for nearly two years, and ultimately insert malicious code resulting in the SUNBURST attack." It next discusses this attack.

According to the Complaint, "the threat actors responsible for SUNBURST accessed SolarWinds' corporate VPN by using an unmanaged third-party device and stolen credentials, exploiting the vulnerability that [SolarWinds' engineer] had identified six months earlier." For approximately two years (from January 2019 until November 2020), the threat actors "conducted reconnaissance, exfiltration, and data collection; identified product and network vulnerabilities; harvested credentials of SolarWinds employees and customers; and planned additional attacks against SolarWinds' products that would be deployed during later stages of the campaign."

Also, in part due to the company's access control deficiencies, 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. The threat actors used multiple accounts that had administrator privileges, exploiting a security problem that SolarWinds had known about since at least June 2017. The threat actors were also able to access and monitor network access and emails of SolarWinds' key personnel without detection. This included exfiltrating approximately 7 million emails from more than 70 SolarWinds employees between approximately December 2019 and December 2020, including emails from the Information Technology and Security groups.

Following months of reconnaissance and data exfiltration from the SolarWinds' networks, in November 2019, the threat actors used information gained from their access to SolarWinds' networks and data to begin a trial run of what ultimately became the SUNBURST attack. The threat actors conducted this trial run by first inserting non-malicious test code into SolarWinds' Orion software builds to determine whether they could successfully evade detection.

Seeing that their insertion of non-malicious code went undetected, in February 2020, the threat actors began inserting malicious code into Orion software builds. Over the next several months, the threat actors inserted malicious code into three different Orion software builds that went out to nearly 18,000 customers. The impacted customers included numerous federal and state government agencies, and more than 1,500 publicly traded U.S. companies, banks, broker-dealers, accounting firms, and other entities regulated by the SEC. . . . The threat actors utilized the SUNBURST attack to conduct additional secondary attacks on approximately 100 of the 18,000 impacted companies and government agencies.

. . . [T]he vulnerabilities that the threat actors exploited to access SolarWinds' system and ultimately infect its customers' systems were vulnerabilities that SolarWinds and Brown had known about for months and that could have been remediated through straightforward

steps.

(Complaint at ¶¶ 138 - 144; emphasis in original.)

SolarWinds and Brown Learned of Attacks on, and Vulnerabilities in, Its Orion Products in 2020

According to the SEC, beginning in early 2020, the Defendants learned of an increase in threats to its products and customers, including multiple attacks against customers' Orion platforms. This intel served as red flags indicating that SolarWinds had been, or was at increased risk of soon becoming, the victim of a significant cyberattack.

The Complaint also discusses how nine of SolarWinds' Managed Service Providers (MSPs),[4] suffered attacks through the MSP product, including ransomware attacks. All of these attacks involved the use of accurate credentials on the threat actors' first attempt, "suggesting that the threat attacks had somehow obtained the credentials before the attack." In March 2020, SolarWinds learned that a threat actor had attacked its MSPs using a list of 19,000 single sign-on customers, "meaning that the threat actors had information to distinguish between customers who had enabled more secure multi-factor authentication and customers who did not have it enabled. This was another red flag that malicious actors had access to SolarWinds' network and/or systems." SolarWinds failed to determine how the threat actors had obtained these credentials though company employees "theorized that it might have been through a breach of SolarWinds' systems." SolarWinds did not publicly disclose any information related to these attacks, update its overall risk disclosure, or identify and remediate the vulnerabilities to render them immaterial.

In June 2020, a Government Agency notified SolarWinds about malicious activity by the Orion software it had installed the previous month and asked SolarWinds to investigate this. SolarWinds' investigation failed to uncover the root cause for the malicious activity or otherwise remediate the vulnerability. The investigation did, however, uncover "'numerous' vulnerabilities - some of which had been present and identifiable for years - that needed to be remedied to protect the Orion platform from future attacks." The large increase in incidents and vulnerabilities led SolarWinds' employees to complain to Brown "that they were inadequately staffed to address the large number of vulnerabilities being identified . . . and that fixing all the issues - even with adequate staff - would take years."

In October 2020, another customer, Firm B, notified SolarWinds about malicious activity on its Orion software. SolarWinds employees recognized that this malicious activity was similar to the activity reported by the Government Agency. Notwithstanding this, SolarWinds "falsely informed Firm B that they had not previously seen similar activity from the Orion platform. In contemporaneous instant messages sent during the telephone call with Firm B, a SolarWinds employee messaged his colleague 'Well I just lied.'" The Complaint continues, "Despite repeated requests from the customer for assistance, SolarWinds again failed to investigate sufficiently, uncover the root cause for the malicious activity, or otherwise remediate the vulnerability in the Orion software, which was being used by thousands of companies worldwide." In the view of the SEC, the failure to disclose these attacks "was part of an overall scheme to conceal both the problems with Orion specifically, and the overall poor state of SolarWinds' cybersecurity" and the Defendants "on multiple occasions, misled customers regarding the quality of its cybersecurity controls to win contracts."

At no point beginning with its IPO in October 2018 did SolarWinds disclose in its SEC filings or elsewhere its numerous cybersecurity risks, vulnerabilities, and incidents affecting its products.

(Complaint at ¶¶ 145 - 165, 175; emphasis in original.)

Once SolarWinds Learned of the SUNBURST Attack, It Did Not Fully Disclose Its Known Impact

In December 2020, a third customer of SolarWinds notified it of an attack against its Orion platform. This customer, Firm C, reverse-engineered the SolarWinds' code to identify what was causing the malicious activity. "Within a matter of days, Cybersecurity Firm C had identified the root cause of the malicious activity within the Orion software code." On December 12, 2020, Firm C contacted SolarWinds Chief Executive Officer and explained that there was a vulnerability in the Orion software as a result of malicious code that had been inserted on the Orion product by a threat actor. The same day, Firm C also shared the decompiled code with SolarWinds during a call with Brown. Apparently, "Brown immediately linked" the three attacks to the same vulnerability.

After the December 12 conversations, Brown and other executives worked to prepare a Form 8-K announcing the vulnerability. This Form was filed on December 14. In the view of the SEC, it "created a materially misleading picture of the Company's knowledge of the impact of the attack." In particular, SolarWinds' disclosure stated 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." According to the SEC, at the time of this disclosure, "SolarWinds knew that this vulnerability was not theoretical but rather . . . it definitely allowed the attacker to compromise the server on which the Orion products were running."

The disclosure also noted that SolarWinds had "hired third-party cybersecurity experts to assist in an investigation of these matters, including 'whether a vulnerability in the Orion monitoring products was exploited as a point of any infiltration of any customer systems.'" At the time, SolarWinds knew that the vulnerability had been exploited as a point of infiltration of customers' systems on at least three occasions. "SolarWinds' disclosure also stated that it was 'still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited'" in any reported attacks. Again, at the time of this statement, "SolarWinds knew the vulnerability in the Orion product had been successfully exploited on at least three prior occasions since as early as May 2020."

(Complaint at ¶¶ 182 - 189.)

According to the Complaint, in addition to documenting violations of the antifraud provisions of the Securities Act of 1933 and of the Securities Exchange Act of 1934, as well as the Defendants repeatedly filing inaccurate and misleading information with the SEC, the above facts document that SolarWinds: had multiple internal control failures; did not have sufficient controls to reasonably protect its critical assets; and, had deficient disclosure controls.[5]

Based upon these violations, the Compliant seeks the sanctions discussed above.

Tamara K. Salmon
Associate General Counsel

Notes

[1] See Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown, Civil Action No. 23-cv-9518 (US SDNY October 30, 2023) (the "Complaint"), which is available at: https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf. A press release the SEC issued about the case is available at: https://www.sec.gov/news/press-release/2023-227.

[2] See Complaint at p. 13.

[3] As discussed in detail in the Complaint, SolarWinds was the subject of the SUNBURST cybersecurity breach (discussed in this memo). The threat actors behind the breach began to access the Defendant's network through a VPN. They remained in their system undetected for approximately two years - until November 2020. Complaint at p. 42.

[4] The MSPs were companies that used SolarWinds' products to provide network management services to end users. These companies often included small or medium-sized firms that wished to outsource their network management.

[5] These violations are discussed in ¶¶ 194-202.
