Cybersecurity Law Report cslawreport.com

Nov. 15, 2023

SEC Enforcement

Navigating SEC Cybersecurity Enforcement in a Post-SolarWinds World

By Jennie Wang VonCannon, *Crowell & Moring*

The Securities Exchange Commission (SEC) has been transparent about how to avoid getting on the wrong side of its cybersecurity-related regulations since wading into the cybersecurity enforcement fray. In March 2022, the SEC proposed rules on cybersecurity risk management, strategy, governance and incident disclosure (Proposed Cybersecurity Rule), citing "ongoing and escalating risk to public companies, investors, and market participants" from cybersecurity threats and incidents. One contributing factor the SEC highlighted was companies' increased reliance on third-party IT services.

After a lengthy comment period, the SEC finalized the Proposed Cybersecurity Rule on July 26, 2023 (Final Cybersecurity Rule). The Final Cybersecurity Rule includes stringent requirements that public companies disclose details about their cybersecurity incidents and enforcement protocols.

The SEC's enforcement approach became yet clearer on October 30, 2023, when it sued IT vendor SolarWinds Corporation (SolarWinds) and its CISO Timothy G. Brown for materially false and misleading statements to SolarWinds' investors about the company's cybersecurity protocols.

Although the SEC's complaint against SolarWinds and Brown was filed after the SEC finalized its Final Cybersecurity Rule, the bottom line is that the more disclosures regarding cybersecurity protocols and incidents there are, the more likely there will be enforcement actions and litigation regarding whether such disclosures violated federal securities and other laws.

This article examines the SEC's complaint against SolarWinds and the company's blog post in response, and discusses five principles that govern the agency's enforcement decisions, providing practical insights to help public and private companies navigate the increasingly fraught regulatory landscape.

See "Navigating the SEC's Newly Adopted Cybersecurity Disclosure and Controls Regime" (Sep. 6, 2023).

The SolarWinds Complaint

On October 30, 2023, the SEC sued SolarWinds and Brown in his individual capacity for securities violations, alleging that both the company and the individual made materially false and misleading statements to SolarWinds investors about the company's cybersecurity protocols. In the two-year period between January 2019 and December 2020, SolarWinds experienced what the SEC calls "one of the worst cybersecurity incidents in history," which caused its stock price to nosedive.

It remains to be seen whether the DOJ will add criminal charges to the SEC action against SolarWinds and Brown.

Policy Violations and False Statements

The SEC made clear in its complaint that it was not charging SolarWinds and Brown for violating federal securities laws simply because the company experienced a "major, targeted cybersecurity attack," which is also known as the SUNBURST attack. Rather, it was SolarWinds' "cybersecurity policy violations, vulnerabilities, and cyberattacks," coupled with the company's and Brown's "materially false and misleading statements and omissions related to SolarWinds' cybersecurity risks and practices in public disclosures, that the SEC said prompted the enforcement action.

Specifically, the SEC alleged that SolarWinds posted a "Security Statement" on its website shortly before its initial public offering in 2018 "tout[ing] the Company's supposedly strong cybersecurity practices," which included claims that the company: "complied with the NIST [National Institute of Standards and Technology] Framework for evaluating cybersecurity practices"; "created its software products in a 'secure development lifecycle' [that] follows standard security practices" such as penetration testing; enforced the use of complex passwords across all of its systems; and set access controls to sensitive data on a "need-to-know/least privilege necessary basis." In reality, the SEC alleged, SolarWinds knew it had "poor cybersecurity practices" and did none of these things.

According to the complaint, SolarWinds also issued SEC filings that were "materially misleading" in that they made "generic and hypothetical" disclosures of the company's cybersecurity risks – lumping them in alongside risks such as "natural disasters, fire, power loss, telecommunication failures . . . [and] employee theft or misuse."

The SEC alleged that Brown – who was "responsible for the overall security program at SolarWinds" and who served as its Vice President of Security and Architecture and head of the Information Security group from July 2017 to December 2020, after which he was promoted to CISO – and other SolarWinds employees knew full well SolarWinds "had serious cybersecurity deficiencies."

See Cybersecurity Law Report's two-part series on digital identity management in a post-pandemic world: "A Framework for Identity-Centric Cybersecurity" (Mar. 24, 2021), and "SolarWinds, Zero Trust and the Challenges Ahead" (Mar. 17, 2021).

Critical Internal Communications

The SEC complaint quotes extensively from SolarWinds employee emails, messages and documents discussing its cybersecurity program. They include, for example:

- Brown's assessment that the company's critical assets were "very vulnerable";
- An engineer's identification of a security vulnerability with SolarWinds' remote access virtual private network – the mechanism that the SEC says malicious actors exploited during the 2019-2020 hack – and warning that it was "not very secure" and could cause "major reputation and financial loss";
- Internal presentations in March and October 2020 that highlighted "[s]ignificant deficiencies" in the company's access controls; and
- A senior information security manager's lament: "[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."

Individual Liability

The fact that Brown was charged by the SEC in his individual capacity alongside the company underscores the U.S. government's continued efforts to hold individuals accountable for cybersecurity-related incidents. It is evidence that the criminal prosecution and conviction of Uber's chief security officer in October 2022 for his handling of two of Uber's data breaches was not a one-off enforcement action, but rather the first of what looks like more to come from the government.

See "Lessons From the Conviction of Uber's Former CISO" (Nov. 9, 2022).

SolarWinds' Response

On November 8, 2023, SolarWinds published a blog post entitled "Setting the Record Straight on the SEC and SUNBURST." In it, the company vehemently denied the SEC's allegations, calling them "false," "fundamentally flawed—legally and factually," and, ironically, "misleading."

Laying Blame at the Victim's Feet

The overall message that SolarWinds sent in its first public response to the SEC's complaint is that the "SEC lacks the authority or competence to regulate public companies' cybersecurity." Despite the SEC asserting that its complaint against SolarWinds was not for the SUNBURST attack, the company sees it differently, stating that "it's unfortunate that the SEC is laying blame for the attack at the feet of its victim." It is, therefore, unsurprising that SolarWinds has come out of the gate swinging, asserting that it will be "fighting this case," and "intend[s] to correct the record and push back on [the SEC's] overreach."

Misleading Allegations

Citing as a "prime example" of the SEC "making inaccurate assertions by twisting the facts," SolarWinds rebuts the SEC's allegations arising out of the company's assertions in its Security Statement that it "follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect and respond to security incidents." The SEC alleged that "SolarWinds met only a small fraction of the cybersecurity controls laid out in the NIST framework and had 'no program/practice in place' for the ***majority*** of the controls. . . ." (emphasis in original). In response, the company criticized the SEC's "supposed evidence" for this claim, which SolarWinds stated was "mainly a preliminary self-assessment from 2019 as to whether SolarWinds met an *entirely different set of standards*" (emphasis in original).

In asserting that the SEC "mix[ed] apples and oranges, underscoring its lack of cybersecurity expertise," SolarWinds drew a distinction between whether it followed the NIST Cybersecurity Framework (which the company maintains it did) and whether it met the standards of NIST Special Publication 800-53 and FedRAMP (which the company appears to concede that it did not "for a small subset of SolarWinds products, which were unaffected by the SUNBURST cyberattack"). Of course, whether the SUNBURST attack affected the company's products is of no moment to the SEC's complaint, which the SEC asserts is targeted at the misleading statements regarding the company's overall cybersecurity regime and not for being a victim of the SUNBURST attack.

Quotes Out of Context

As for the employee communications quoted in the SEC complaint, SolarWinds' response is that the SEC "misleadingly quotes snippets of documents and conversations out of context to patch together a false narrative about [the company's] security posture." Through its blog post, the company is telegraphing that its defense against the SEC's allegations will include the argument that SolarWinds did have adequate cybersecurity controls and, as such, its statements were neither false nor misleading. While on the one hand the SEC calls the attack "one of the worst cybersecurity incidents in history," the company's rebuttal is that "SUNBURST is widely regarded as one of the most sophisticated cyberattacks of all time." Both statements are not mutually exclusive, and it remains to be seen whether the company's cybersecurity protocols will be deemed to have made it particularly vulnerable to the attack attributed to Russia.

Standard Regulatory Filings

SolarWinds disputes the SEC's allegations that its regulatory filings were misleading. The company maintains that its risk disclosure "was comparable to those of leading U.S. technology companies," arguing that "if [SolarWinds'] risk disclosure were [*sic*] considered inadequate, everyone's risk disclosures would be inadequate." While that very well may be true, the fact remains, however, that the SEC chose to file an enforcement action against SolarWinds and not, as yet, everyone else. The accuracy of SolarWinds' SEC filings will be analyzed in the context of the company's own cybersecurity controls, so the "everyone else was doing it" defense may not carry the day.

See "Takeaways From the SEC's Enhanced Cybersecurity Disclosure Regime for Public Companies" (Apr. 6, 2022).

SEC's Enforcement Principles Offer Key Takeaways

A month before the SEC released the Final Cybersecurity Rule, its Director of the Division of Enforcement, Gurbir S. Grewal, spoke to an audience of policymakers, financiers and corporate leaders attending the Financial Times Cyber Resilience Summit in Washington, D.C., on June 22, 2023. Director Grewal promulgated five principles that govern the SEC's enforcement decisions.

In light of the SEC's recent complaint against both SolarWinds and its CISO, regardless of how the action is resolved, these principles are particularly instructive to public and private companies navigating the increasingly fraught regulatory landscape when it comes to cybersecurity.

Principle #1: Make Timely and Accurate Disclosures

The SEC considers investors to be the victims of cyberattacks on publicly traded companies, so its goal is to "prevent *additional* victimization by ensuring that investors receive timely and accurate required disclosures," Grewal stated.

When a public company suffers a cyber breach, it should remember that the real-time decisions it makes to respond to such a breach "directly impact customers whose PII or financial information ha[ve] been compromised" and "may also be material to investors in publicly traded companies."

Accordingly, the company must make timely disclosures about the breach, the company's response, and its impact to customers and investors. In the context of the Final Cybersecurity Rule, this means that a company must – while in the throes of a cyber incident – determine whether such incident is "material" to investors, and then disclose that incident within 96 hours. This is clearly going to be a tall order, and companies would be well-served to have a handle on the total mix of information made available to the investing public at any given time so the analysis of whether an individual cyber incident is material can be conducted more efficiently.

See "SEC Chair Gensler's Stance on Three Key Disclosure Areas and the Role of Individual Accountability in Enforcement Actions" (Jan. 12, 2022).

Principle #2: Implement Real Policies

Companies "need to have *real* policies that work in the *real* world, and then they need to actually *implement* them"; firms "paying lip service" to their cybersecurity programs are more likely to face enforcement action, according to Grewal.

The SEC warns that "having generic 'check the box' [cybersecurity policies]" is not going to cut it. In other words, the SEC wants to see granularity in companies' policies that guide its employees in

how to identify security red flags, and how to respond to those flags once they are identified. Companies should take a practical approach to drafting cybersecurity policies by thinking through how such policies will be implemented by real-life employees.

Principle #3: Keep Cybersecurity Policies Up to Date

Cybersecurity policies must be kept up to date to "keep up with constantly evolving threats," stressed Grewal.

In keeping with the SEC's emphasis on companies' timely and accurate disclosures to the investing public, companies should regularly review and update their cybersecurity policies because cyber threats are constantly evolving. Notably, the SEC advises companies *and their counsel* to review the SEC's cybersecurity-related enforcement actions and public orders because "they clearly outline what good compliance looks like and where and how registrants fall short with their cybersecurity obligations."

The SolarWinds complaint, then, indicates that the SEC believes that if a company's own employees apparently do not believe in its cybersecurity program, then the company should proceed with caution in touting its strengths in public statements or regulatory filings.

See "Updating Cyber Policies to Align With Recent SEC Exams and Guidance" (Nov. 13, 2019).

Principle #4: Report Cyber Incidents Up the Chain

When a cyber incident happens, "the right information must be reported up the chain to those making disclosure decisions," Grewal instructed.

Cybersecurity policies are limited to words on paper. In practice, the "right information" needs to be delivered to leaders making decisions in accordance with those policies and applicable regulations. According to the SEC, this means that if information security personnel become aware of a cyber vulnerability, they need to report it up the chain so that the company's executives are not "in the dark" for months, Grewal said.

See "Incident Response in the Financial Services Industry" (Jul. 28, 2021).

Principle #5: No Gamesmanship Around Disclosures

The SEC has "zero tolerance for gamesmanship around the disclosure decision," Grewal warned. Specifically, the following behaviors are likely to draw the SEC's ire: being more concerned with reputational damage than "coming clean with shareholders," "stick[ing] their head in the sand," adopting "hyper technical readings of the rules" or "minimizing the cyber incident."

Companies would be well-served in assuming, as the SEC does, that it is nearly impossible to keep the existence of a cyber breach secret, and proceed accordingly in complying with their attendant disclosure obligations – which are now much more stringent in light of the SEC's Final

Cybersecurity Rule. The SEC advises registrants to "come and talk to us sooner rather than later – not in six months after you finish your internal investigation." Director Grewal emphasized that "firms that meaningfully cooperate with an SEC investigation, including by coming in to speak with us or self-reporting, receive real benefits, such as reduced penalties or even no penalties at all."

See Cybersecurity Law Report's two-part series on SEC cybersecurity disclosure enforcement: "Recent Developments" (Sep. 22, 2021), and "Best Practices" (Sep. 29, 2021).

Jennie Wang VonCannon is a partner in Crowell & Moring LLP's Los Angeles office. She is a trial lawyer and advisor with extensive experience and deep understanding of corporate defense in both criminal and civil contexts, cybersecurity and intellectual property matters. Her 11 years as a federal prosecutor culminated in her selection to serve with distinction as the Deputy Chief of the Cyber and Intellectual Property Crimes Section of the National Security Division of the U.S. Attorney's Office for the Central District of California. Prior to becoming a federal prosecutor, she was a securities litigator.