WINSTON & STRAWN LLP

BLOG

SEC Charges Four Companies With Misleading Cyber Disclosures on SolarWinds Hack

OCTOBER 30, 2024

On October 22, 2024, the Securities and Exchange Commission (the SEC) announced charges and million-dollar penalties against four companies for allegedly making materially misleading disclosures regarding cybersecurity risk and intrusions relating to SolarWinds' Orion software hack. SolarWinds provides an IT performance and monitoring product called Orion, which issued a routine software update in March 2020. In early 2021, it was reported that hackers had slipped malicious code into the Orion software update and used it to access the networks, systems, and data of thousands of SolarWinds customers.

THE CHARGES

Four companies were accused of negligently minimizing the impact of the SolarWinds hack in their public disclosures, with one company also being charged with failing to maintain adequate disclosure controls and procedures as required by the Sarbanes-Oxley Act of 2002 (SOX).

All four companies agreed to pay civil penalties to settle the charges:

- One company will pay a $4 million civil penalty. The SEC's order found that the company described risks from cybersecurity events in its filings as hypothetical, despite knowing that two SolarWinds-related intrusions exfiltrated gigabytes of data. The order also found that these materially misleading disclosures resulted in part from the company's deficient disclosure controls.
- Another company will pay a $1 million civil penalty. The company stated in its filings that the threat actor accessed a "limited number of [the] Company's email messages," when the company knew, and did not disclose, that the threat actor had also accessed at least 145 files in its cloud file sharing environment, some of which contained sensitive company information.
- Another company will pay a $995,000 civil penalty. The SEC's order states that, despite knowing about the cybersecurity compromise, the company described the intrusion and risks in its filings in generic terms similar to those in previous filings and omitted new and material risks.
- Another company will pay a $990,000 civil penalty. The SEC's order found that the company minimized the attack by failing to disclose the number of customers whose credentials were accessed, the nature of the code that the threat actor exfiltrated, and the quantity of encrypted credentials that the threat actor accessed.

The orders found that each of the companies violated certain provisions of the Securities Act of 1933, the Securities Exchange Act of 1934, and related rules thereunder. None of the four companies involved have admitted or denied the SEC findings, but all have voluntarily taken steps to enhance cybersecurity controls in the wake of the investigation.

KEY TAKEAWAYS

The charges serve as a reminder that "federal securities laws prohibit half-truths, and there is no exception for statements in risk-factor disclosures," as stated by Jorge G. Tenreiro, Acting Chief of the SEC's Crypto Assets and Cyber Unit. He noted that "downplaying the extent of a material cybersecurity breach is a bad strategy."

Sanjay Wadhwa, Acting Director of the SEC's Division of Enforcement, said that the companies' actions left investors in the dark about the true extent of the incident. He stated that the "enforcement actions reflect [that] while public companies may become targets of cyberattacks, it is incumbent upon them to not further victimize their shareholders or other members of the investing public by providing misleading disclosures about the cybersecurity incidents they have encountered."

The charges demonstrate that cybersecurity is an SEC enforcement priority, and the SEC may continue to focus on negligence-based fraud related to unreported or underreported cyber-attacks. To avoid similar penalties, companies should have an incident response procedure and a disclosure policy in place, as disclosure and escalation procedures are vital in the wake of a cybersecurity attack, and ensure that such disclosure controls and procedures are adequate under SOX. Companies should also review their disclosures and risk factors related to cybersecurity to ensure that they are fully complying with the rules under the Securities Act of 1933 and the Securities Exchange Act of 1934.

Winston's Capital Markets and Securities Law Watch will continue to monitor developments in this area and will provide our readers with updates.

Associate Meg Thomas also contributed to this blog post.

3 Min Read

Authors

David A. Sakowitz

Ben D. Smolij

Emily Semon

Meg Thomas

Related Topics

Cyber Disclosure | Cyber Security | Enforcement | Government Investigations & Enforcement | Securities and Exchange Commission (SEC) | Securities Act of 1933 | Securities Exchange Act

Related Capabilities

Capital Markets | Public Companies | Corporate Governance

Government Investigations, Enforcement & Compliance

Related Professionals

David A. Sakowitz

Ben D. Smolij

Emily Semon

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.

© 2024 Winston & Strawn LLP.