Published on *The National Law Review* https://natlawreview.com

SEC Charges Against SolarWinds Signal Resolute Cybersecurity Enforcement and May Spur Surge in Cybersecurity Whistleblowing to SEC

Article By:

Jason Zuckerman

Matthew Stock

Today the SEC filed a complaint against SolarWinds Corporation and its CIO for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities. According to the complaint, SolarWinds defrauded investors by overstating its cybersecurity practices and understating or failing to disclose known risks. The SEC's complaint signifies robust SEC enforcement of cybersecurity-related securities violations, including failure to disclose known material cybersecurity risks and failure to maintain adequate cybersecurity controls. In a press release announcing the charges, Gurbir S. Grewal, Director of the SEC's Division of Enforcement, states: "Today's enforcement action not only charges SolarWinds and Brown for misleading the investing public and failing to protect the company's 'crown jewel' assets, but also underscores our message to issuers: implement strong controls calibrated to your risk environments and level with investors about known concerns."

In light of the elevated cybersecurity risk environment and the SEC prioritizing enforcement of cybersecurity violations, cybersecurity whistleblowers have a strong incentive to report cybersecurity violations to potentially qualify for an SEC whistleblower award and can play a vital role in protecting against cyber breaches and attacks.

Information security and data privacy whistleblowers are often in a position to identify and remedy vulnerabilities—and therefore prevent breaches—if only decision makers would act on their concerns. In our practice representing cybersecurity whistleblowers, we find that all too often, chief information security officers and other information security professionals encounter indifference or retaliation when they raise concerns about vulnerabilities. The SEC whistleblower program offers a powerful incentive for cybersecurity whistleblowers to report violations to the SEC and assist the SEC in taking decisive enforcement actions that will encourage registrants to provide accurate disclosures about cybersecurity and maintain appropriate cybersecurity controls.

This post discusses the implications of the charges against SolarWinds and how cybersecurity whistleblowers can qualify for an SEC whistleblower award.

SEC Complaint Against SolarWinds

The complaint alleges what appears to be a blatant failure to remedy significant cybersecurity vulnerabilities and concealment from shareholders of the risks stemming from those vulnerabilities:

- SolarWinds allegedly misled investors by disclosing only generic and hypothetical risks at a time when the company and its CIO knew of specific deficiencies in SolarWinds' cybersecurity practices.
- SolarWinds' public statements about its cybersecurity practices and risks were at odds with its internal assessments, including internal emails and presentations revealing that SolarWinds was aware that the "current state of security leaves [it] in a very vulnerable state for [its] critical assets," "[a]ccess and privilege to critical systems/data is inappropriate," "backends are not that resilient," "the volume of security issues being identified . . . outstripped the capacity of Engineering teams to resolve," and "[t]he products are riddled and

obviously have been for many years."

- SolarWinds concealed from the public its known poor cybersecurity practices, including its (a) failure to consistently maintain a secure development lifecycle for software it developed and provided to thousands of customers, (b) failure to enforce the use of strong passwords on all systems, and (c) failure to remedy access control problems that persisted for years.
- SolarWinds knew about a "security gap" relating to its VPN, which allowed access from devices not managed by SolarWinds. A network engineer warned that someone exploiting the vulnerability "can basically do whatever without us detecting it until it's too late."
- SolarWinds' Security Statement contained multiple materially false and misleading statements. It contained positive information about the state of the Company's cybersecurity practices while failing to include information such as the fact that SolarWinds failed to meet more than half of NIST standards.
- When SolarWinds filed a Form 8-K first announcing that its Orion network monitoring software contained malicious code that had been inserted by threat actors as part of a supply-chain attack, it failed to disclose that the vulnerability at issue had been actively exploited against SolarWinds' customers multiple times over at least a six-month period.

The complaint reveals how the SEC applies anti-fraud and internal control rules to cybersecurity violations, including two key issues:

- The SEC is willing to take enforcement action for failure to disclose cybersecurity vulnerabilities in the absence of a breach or attack. The complaint states: "To be clear, SolarWinds' poor controls, Defendants' false and misleading statements and omissions, and the other misconduct described in this Complaint, would have violated the federal securities laws even if SolarWinds had not experienced a major, targeted cybersecurity attack."
- Generic rusk disclosures about hypothetical cybersecurity risks will not suffice when a company is aware of elevated risks and omits those risks from its disclosures. Here, SolarWinds documented internally that "current state of security leaves [it] in a very vulnerable state for [its] critical assets," but it did not disclose those risks to

shareholders. The complaint states: “SolarWinds’ disclosures failed to convey the known risks discussed above, or even that known risks of this type had been identified. Even if some of the individual risks and incidents discussed in this Complaint did not rise to the level of requiring disclosure on their own, at least collectively they created such an increased risk to SolarWinds that the failure to disclose their collective impact on SolarWinds’ cybersecurity posture rendered the risk disclosures that SolarWinds made materially misleading.”

Cybersecurity Securities Violations

The complaint against SolarWinds alleges violations of the following provisions of federal securities laws:

- the antifraud provisions of the Securities Act of 1933 (Section 17(a) of the Securities Act,15 U.S.C. § 77q(a));
- the antifraud provisions of the Securities Exchange Act of 1934 (Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5(b), 17 C.F.R. § 240.10b-5);
- the reporting and internal controls provisions of the Exchange Act (Section 13(a) of the Exchange Act, 15 U.S.C. § 78m(a)] and Rules 13a-1, 13a-11, and 13a-13 thereunder, 17 C.F.R. §§ 240.13a-1, 240.13a-11, and 240.13a-13), which require issuers to file accurate reports on Forms 10-K, 10-Q, and Form 8-K;
- Section 13(b)(2)(B) of the Exchange Act, 15 U.S.C. § 78m(b)(2)(B), which requires registrants to devise and 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; and
- Exchange Act Rule 13a-15(a) which requires publicly traded companies to maintain disclosure controls and procedures to ensure that information required to be disclosed by an issuer is accumulated and communicated to the issuer’s management to allow timely

decisions regarding required disclosure.

In December 2023, the SEC will have an additional tool to combat cybersecurity violations in that the recently adopted rules on cybersecurity risk management, strategy, governance, and incident disclosure will become effective. These rules require registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance.

New Form 8-K Item 1.05 will require registrants to disclose any cybersecurity incident they determine to be material and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the registrant. And new Regulation S-K Item 106 will require registrants to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats and describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats. The new Regulation S-K Item 106 will be effective for annual reports for fiscal years ending on or after December 15, 2023 and the incident disclosure requirements in Form 8-K Item 1.05 will become effective around December 18, 2023.

SEC Whistleblower Awards for Cybersecurity Whistleblowers

Under the SEC Whistleblower Program, the SEC is required to pay awards to eligible whistleblowers who voluntarily provide the SEC with original information that leads to a successful enforcement action resulting in monetary sanctions in excess of $1 million.

A cybersecurity whistleblower may receive an award of between 10% and 30% of the total monetary sanctions collected. If represented by an attorney, a whistleblower may submit a tip anonymously to the SEC.

Since 2012, the SEC has issued more than $1.8 billion in awards to whistleblowers. SEC whistleblower attorneys can provide critical guidance to whistleblowers throughout this process to protect their identities and increase the likelihood that they not only obtain, but maximize, their awards. See our tips to obtain an SEC whistleblower award.

Federal and state whistleblower protection laws protect cybersecurity whistleblowers against retaliation, including the Sarbanes-Oxley Act, the False Claims Act, and the Defense Contractor Whistleblower Protection Act.

National Law Review, Volumess XIII, Number 304

Source URL:https://natlawreview.com/article/sec-charges-against-solarwinds-signal-resolute-cybersecurity-enforcement-and-may