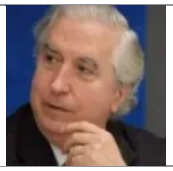

John C. Coffee, Jr. – Mass Torts and Corporate Strategies: What Will the Courts Allow?

By John C. Coffee, Jr.

Compliance's Next Challenge: Polarization

By Miriam H. Baer

Will the Common Goo Guys Come to the Shootou in SEC v. Jarkesy? And Why It Matters

By Eric W. Orts

Editor-At-Large
Reynolds Holding

THE CLS BLUE SKY BLOG

COLUMBIA LAW SCHOOL'S BLOG ON CORPORATIONS AND THE CAPITAL MARKETS

Editorial Board
John C. Coffee, Jr.
Edward F. Greene
Kathryn Judge

Skadden Discusses What SEC's Solar Winds Complaint Means for Boards, Information Security Officers

By Anita Bandy, William Ridgway, David Simon, Joshua Silverstein and Shirley Diaz November 13, 2023

Comment

On October 30, 2023, the SEC filed a litigated complaint against SolarWinds, a software development company, and Timothy Brown, its chief information security officer (CISO). The SEC alleges that from October 2018, when SolarWinds went public, to January 2021, SolarWinds and Brown made materially misleading statements and omissions about the company's cybersecurity practices and risks in public disclosures, which the SEC claims ultimately led to a drop in SolarWinds' stock following the later disclosure of a large-scale cybersecurity attack known as SUNBURST.

Specifically, the complaint alleges that SolarWinds and Brown inaccurately claimed on a website security statement that the company followed cybersecurity standards like the National Institute of Standards and Technology Cybersecurity Framework (NIST framework), used Secure Development Lifecycle (SDL) practices, enforced strong password policies and maintained adequate access controls. Further, the SEC alleges that SolarWinds's periodic filings included generic and hypothetical cybersecurity risk statements that failed to address known risks. Finally, the SEC alleges that, at the time of drafting the Form 8-K filed on December 14, 2020, disclosing the SUNBURST cybersecurity incident, SolarWinds and Brown knew of several confirmed attacks against customers, yet drafted the 8-K to frame the vulnerability as hypothetical.

The SEC also accused SolarWinds of having deficient cybersecurity controls and known vulnerabilities that left its systems susceptible to attack. Internal documents allegedly warned about these cybersecurity gaps, but the company's statements purportedly concealed cybersecurity failings that were then exploited in the SUNBURST cyberattack in late 2020 and impacted Orion software used by thousands of SolarWinds customers. Before the attack, SolarWinds and Brown purportedly knew about vulnerabilities and attacks involving Orion, but they were not disclosed.

The SEC's complaint charges SolarWinds and Brown with direct anti-fraud violations for alleged misstatements as well as direct and secondary liability against them for internal controls violations. This case marks a significant precedent, as it is the first instance where the SEC charged a CISO with fraud, representing a profound departure from its traditional focus on officers with explicit accounting and disclosure duties and SEC reporting expertise. This unprecedented action highlights the increasing importance of cybersecurity in the realm of federal securities law and underscores the gravity of the role CISOs play in the accurate representation of a company's cyber health. The SEC's complaint seeks not only corrective actions but also significant penalties, including injunctions, the return of ill-gotten gains and a prohibition on Brown serving as an officer or director in any public company, reflecting the severity with which the agency views these alleged infractions.

What CISOs Need To Know

The SEC's complaint names Brown individually and serves as a stark reminder to CISOs about the consequences of public and internal statements regarding cybersecurity practices and risks. The complaint highlights the expectation for CISOs to provide accurate representations of their company's cybersecurity posture both internally and in public disclosures. The SEC's detailed complaint against Brown provides insight into the specific practices that CISOs should keep in mind:

- **Carefully Review Public Statements and Disclosures:** The SEC alleges that SolarWinds' CISO provided sub-certifications that inaccurately attested to the company's cybersecurity controls, which were then relied upon in the company's SEC filings. This scenario underscores the heightened responsibility CISOs have, especially when involved with Sarbanes-Oxley Act (SOX) certification processes. In such cases, CISOs face an increased risk that the SEC will hold them to a higher standard for purposes of assessing the company's disclosures and internal controls environment. CISOs should verify that public disclosures align with internal realities and are based on a thorough understanding of the company's cybersecurity posture.
- **Implement and Follow Robust Policies and Procedures:** The SEC's complaint alleges that SolarWinds claimed adherence to cybersecurity standards like the NIST framework without actual implementation. CISOs should not only advocate for the adoption of recognized cybersecurity practices but also ensure they are fully implemented and adhered to throughout the organization.

- **Escalate Known Security Issues Promptly:** The SEC alleged that Brown did not disclose or act on vulnerabilities that network engineers raised to him in a timely manner. CISOs must establish clear channels and protocols for escalating critical cybersecurity issues to ensure that senior management and the board are informed in real time, allowing for proper disclosures.
- **Consider the Scope of Director and Officer Insurance Coverage:** The SEC's action against Brown highlights the personal risk CISOs face when disclosures are inaccurate. CISOs should evaluate their own liability and ensure they have adequate D&O insurance coverage. This may not be available where the CISO is not an actual officer, and coverage may not reach findings of fraud.
- **Document Internal Discussions, Decisions and Judgment Calls:** The complaint suggests that there was a lack of proper documentation regarding the actual cybersecurity risks at SolarWinds as described in periodic filings. CISOs should consider keeping detailed records of key discussions and decisions related to cybersecurity risks, especially when the decisions assess the question of materiality of a particular breach or cyber incident.

The SEC's focus on the accuracy of cybersecurity-related statements made by CISOs emphasizes the critical role they play in a company's compliance with federal securities laws. CISOs must ensure that there is no significant disconnect between what is being communicated publicly and the actual cybersecurity challenges the company faces. The increasing trend of regulatory scrutiny over such matters makes it essential for CISOs to adopt a proactive approach to their company's cybersecurity disclosures. For more insights on this topic, see our November 3, 2023, client alert "Private Equity CISO Fireside Chat — Cybersecurity Leadership in the Age of Generative AI."

What the Board and Senior Executives Need To Know

The SEC's complaint against SolarWinds, along with previously filed SEC actions, places increased emphasis on the responsibility of boards to ensure accuracy and integrity in cybersecurity disclosures:

- **Proactive Vulnerability Management and Disclosure:** Boards must ensure that internal cybersecurity weaknesses, once identified, are promptly addressed with adequate resources and that these vulnerabilities are timely raised to disclosure counsel. In June 2021, the SEC brought a case against First American Financial Corporation for disclosure controls and procedures violations related to a cybersecurity vulnerability that exposed sensitive customer information, even though the vulnerability was not exploited. The SEC found that, by the time senior executives filed an 8-K related to the vulnerability, several months had passed since the company's information security personnel had identified it, but the personnel had not informed senior executives of the vulnerability and failed to remediate it in accordance with the company's policies. The SEC found this information gap to reflect a failure to maintain disclosure controls and procedures.
- **Validate Cybersecurity Assurances:** Assurances made publicly regarding cybersecurity must be defensible and consistent with the reality of the company's cyber health, as reflected by the SEC's actions against SolarWinds.
- **Understanding the Weight of Cumulative Cyber Risks:** It is crucial for boards to recognize that individual cybersecurity issues, while perhaps not material on their own, can aggregate to a level of significance that necessitates disclosure. The board should also assess the need for disclosures of prior incidents to provide context for current incidents, ensuring that the full picture of cyber risk is conveyed to investors.
- **Involvement of CISO in Disclosure Committee:** Given the technical nature of cybersecurity risks, the SEC's focus on the role of SolarWinds' CISO suggests that boards should consider the involvement of CISOs in the disclosure process to improve the quality and accuracy of SEC filings.
- **Understanding the SEC's Expansive View of Materiality:** Traditionally, the SEC considered the materiality of an event based on a quantifiable financial impact. More recently, the agency has taken a more expansive view on materiality, focusing increasingly on qualitative rather than quantitative factors. Therefore, boards and executives must consider qualitative factors when assessing a cybersecurity event, regardless of insurance coverage. Considerations should include:
  - The extent to which the attack uncovers significant deficiencies in the company's cybersecurity infrastructure.
  - Any potential implications for systems associated with SOX compliance and financial reporting, including the integrity of the information processed by these systems.
  - The scope of sensitive customer or employee data compromised.
  - Costs relating to remediation.
  - Loss of a material contract or customer business.
  - Reputational harm.
  - Stock impact from when an announcement was made.
- **Distinguishing Actual From Hypothetical Risks in Disclosures:** In the aftermath of the SolarWinds attack, the SEC criticized the company's Form 8-K for framing known vulnerabilities as hypothetical. This was also seen in the cases against Blackbaud Inc. and Pearson plc, where actual incidents were not appropriately disclosed, leading to SEC charges. Boards should direct the formulation of 8-K disclosures to specifically and accurately distinguish between actual cyber events and potential, hypothetical risks. This includes avoiding language that downplays known exploits or vulnerabilities as merely possible or speculative when there is concrete evidence to suggest otherwise.

Boards are encouraged to reexamine their disclosure practices and ensure that the company's public statements are accurate reflections of its internal situation. The board should work closely with the CISO and legal and compliance teams to develop a clear and defensible reporting strategy that considers the actual status of cybersecurity risks and incidents. The SEC's actions in the SolarWinds case and others serve as a clear warning that inaccuracies or mischaracterizations in such disclosures can lead to significant legal and reputational repercussions.

This post comes to us from Skadden, Arps, Slate, Meagher & Flom LLP. It is based on the firm's memorandum, "What Does the SEC's Complaint Against SolarWinds Mean for CISOs and Boards?" dated November 3, 2023, and available here.