Blogs
November 08, 2024

In late October, the SEC announced settled enforcement actions against four public companies, all stemming from impacts from the compromise of SolarWinds' Orion software. Each order included allegations that the applicable company provided materially misleading statements and/or omissions regarding its cybersecurity risks and incidents related to the compromise of SolarWinds' software. One also alleged violations related to disclosure controls and procedures. The civil penalties to be paid by the companies ranged from $990,000 to $4 million.

Commissioners Hester Peirce and Mark Uyeda issued a dissenting statement in connection with the orders, arguing that the proceedings reflect "a hindsight review to second-guess the disclosure" that "cites immaterial, undisclosed details to support" the charges. The concerns raised by Commissioners Peirce and Uyeda include the

following:

- Inconsistent with the cybersecurity disclosure rules (which were adopted after the events and disclosures relevant to these orders), the enforcement actions called out the companies for failing to provide "details regarding the incident itself" rather than the "impact" of the incident.
- These proceedings might make companies believe they need to "fill their Item 1.05 disclosures with immaterial details about an incident, or worse, provide disclosure under the item about immaterial incidents."
- The position taken in the proceedings regarding updating cybersecurity risk factors following a cybersecurity incident tracks the SEC's arguments in the SolarWinds case in district court, which the court rejected. The dissenting statement notes that "[t]he court rejected the argument after a detailed review of SolarWinds' risk disclosure and concluded that '[v]iewed in totality, [such] disclosure was sufficient to alert the investing public of the types and nature of cybersecurity risks SolarWinds faced and the grave consequences these could present for the company's financial health and future.'"

These views from Commissioners Peirce and Uyeda may strongly indicate the direction in which SEC enforcement will trend under the incoming presidential administration. Even if SEC enforcement changes direction for the next few years, it's worth paying attention to these enforcement actions as they remain thematically consistent with SEC pronouncements spanning multiple administrations (including guidance issued in 2018). Continuing themes include the following:

- If your company experiences a cybersecurity incident, review cybersecurity risk disclosures and consider whether any updates are appropriate. A common issue, which was addressed in one of the enforcement actions, is discussing cybersecurity risks in hypothetical terms after the company has experienced such an incident. Companies should also be thinking about reviewing and updating their Form 10-K cybersecurity disclosures under the requirements that went into effect last year in light of new threats, risks, and incidents.
- What information is material is likely to vary across incidents and companies. All four enforcement actions argue that failure to disclose certain details about the incidents obscured the importance of the events to the business and operations of the companies, including the extent of customer data and company code affected. The orders seemed to focus on these particulars because the subject companies were all in the software or information technology industries. Despite the criticisms from Commissioners Peirce and Uyeda, it is worthwhile for companies to consider what information may be necessary to disclose in order to paint a fulsome picture of the impacts of an incident.
- Most public companies reviewed, and many updated, their controls and procedures following last year's adoption of the cybersecurity disclosure rules. Given the constantly changing nature of cybersecurity threats and risks, it is always worth a reminder to confirm that incident information makes its way to disclosure decision-makers.

Authors

Allison C. Handy

Partner
AHandy@perkinscoie.com 206.359.3295
Blog series

Public Chatter

Public Chatter provides practical guidance—and the latest developments—to those grappling with public company securities law and corporate governance issues, through content developed from an in-house perspective.

View the blog