POLSINELLI

Publications

November 4, 2024 • Updates

SEC Penalties Relating to Cybersecurity Disclosures

On October 22, 2024, the Securities and Exchange Commission ("SEC") charged four current or former publicly traded companies with disseminating materially misleading disclosures regarding cybersecurity risks and actual infiltrations. The charges arose from an investigation of companies impacted by the well publicized 2020 cybersecurity incident involving SolarWinds Corporation's flagship Orion software platform.

The SEC charged that each of these companies learned in either 2020 or 2021 that the perpetrator of the SolarWinds Orion cyberattack had also infiltrated their respective systems, but in their respective public disclosures in 2021 and/or 2022, each company negligently minimized the impact of the cybersecurity incident.

The SEC Staff reiterated its position that, although public companies may be victims of cyberattacks, they may not harm their shareholders or the investing public by issuing misleading disclosures about such cybersecurity incidents. The SEC alleged that each company violated Section 13(a) of the Securities Exchange Act of 1934, as amended, as well as the respective rules promulgated thereunder that require public companies to file annual, quarterly and current reports in conformity with the SEC's rules and regulations.

The companies agreed to settle the SEC's charges as follows:

- Company A agreed to a $990,000 civil penalty
    - In multiple Forms 8-K filed in 2021, Company A minimized the severity of the attack on it by, among other things, failing to disclose the quantity of encrypted credentials accessed by the threat actor
- Company B agreed to a $1 million civil penalty
    - Company B disclosed in a Form 10-Q filed in February 2021 that the threat actor had accessed a limited number of email messages; in reality, Company B was already aware the threat actor accessed over 100 files in its cloud file sharing environment
- Company C agreed to a $995,000 civil penalty
    - Even though Company C was aware of the intrusion, it described cyber intrusions and related risks in a generic fashion in its Annual Reports on Form 20-F filed in both 2021 and 2022
- Company D agreed to a $4 million civil penalty

Related People

- Eric S. Wu
- Pavel (Pasha) A. Sternberg
- Mary Ann H. Quinn

Related Capabilities

- Privacy & Cybersecurity
- Securities & Corporate Finance
- SEC Disclosure, Corporate Governance & Listed Company Compliance

- Company D described its risks from hypothetical future cybersecurity events in its Annual Reports on Form 10-K filed in both 2021 and 2022, even though it was aware it had already experienced two intrusions related to SolarWinds
- In addition, the SEC charged Company D with violations relating to disclosure controls and procedures, resulting in such materially misleading disclosures

The latter two companies, in particular, did not comply with SEC Staff guidance articulated in 2011 and 2018 that registrants refrain from drafting cybersecurity risk factors as hypothetical or generic when already aware that those risks had fully materialized.[1] [2]

At the time of the SolarWinds incident, ransomware was just beginning to enter the public consciousness. Since then, cybersecurity attacks have become more sophisticated and at the same time more common. Ransomware attacks and widespread third-party incidents have especially gained prominence as companies increasingly grapple with vendor risk management and supply chain attacks. In part because of the "success" of those attacks, ransomware is now one of, if not the most, common type of attack companies experience. Attacks on vendors that are focal points in a particular industry or that act as a key point in a supply chain can cripple an entire sector of the economy or simultaneously provide hackers with access to data or networks of a wide range of companies. Examples of supply chain attacks are the 2023 MoveIt vulnerability that compromised the data of hundreds of organizations and the June 2024 CDK Global attack, which disrupted auto sales nationwide.

As cybersecurity attacks have become more prevalent, the reporting obligations have also expanded. In July 2023, the SEC adopted new cybersecurity disclosure rules, which create more prescriptive data security incident disclosure requirements. Significantly, a "material cybersecurity incident" now must be disclosed under Item 1.05 of Form 8-K within four business days of the date such cybersecurity incident is determined to be material. For more information about those rules see our client alert from July 2023.

While any cybersecurity attack can create challenges to comply with the SEC's reporting obligations, especially in light of the new requirement to disclose within four business days of a materiality determination, the ransomware and vendor focused attacks present unique challenges. In the case of a ransomware attack, assessing the incident and communicating about it publicly can be very difficult when an organization is trying to recover from the attack and restore operations. And, in the case of a vendor incident, the lack of access to the compromised network and the often limited information about the incident makes accurately reporting an incident challenging.[3]

The SEC's 2023 rulemaking and its actions described above illustrate its continued focus on public companies' cybersecurity disclosures. Accordingly, reporting companies should review their disclosure controls and procedures to confirm their effectiveness in enabling compliance with the SEC's cybersecurity disclosure rules in connection with future cybersecurity incidents that may impact them directly or indirectly. If you have any questions regarding the matters covered in this publication, please contact any of the authors or another member of your Polsinelli team.

[1] In the 2018 Commission Statement and Guidance on Public Company Cybersecurity Disclosure (SEC Release Nos. 33-10459; 34-82746), the SEC's interpretive guidance specified that ". . . if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur . . . Instead, the company may

need to discuss the occurrence of that cybersecurity incident and its consequences . . .”

[2] In the 2011 SEC Division of Corporation Finance Disclosure Guidance: Topic No. 2, the Division specified that “. . . if a registrant experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur.”

[3] The July 2023 adopting release clarifies that “the definition of ‘information systems’ contemplates those resources owned by third parties and used by the registrant” (SEC Release Nos. 33-11216; 34-97989, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*). As such, a third-party incident may result in a material cybersecurity incident for a reporting company.