LEGAL UPDATES

PUBLISHED: NOVEMBER 25, 2024

SEC Charges Public Companies with Misleading Cyber Disclosures

Service

Securities & Corporate Governance

Professionals

STEVEN R. BARRETT
CHATTANOOGA:
423.757.5905
STEVE.BARRETT@
HUSCHBLACKWELL.COM

ROBERT J. JOSEPH
CHICAGO:
312.526.1536
ROBERT.JOSEPH@
HUSCHBLACKWELL.COM

ANDREW SPECTOR
BOSTON:
617.598.6700
ANDREW.SPECTOR@
HUSCHBLACKWELL.COM

ANNORAH HARRIS
ST. LOUIS:
314.480.1983
ANNORAH.HARRIS@
HUSCHBLACKWELL.COM

On October 22, 2024, the Securities and Exchange Commission (SEC) announced that it had charged four companies with making materially misleading disclosures regarding cybersecurity risks and intrusions, with one company also charged with disclosure controls and procedures violations. None of the orders specifically cite the new cybersecurity disclosure rules which went into effect in 2023 (a summary of which can be found here) because the conduct in question occurred prior to the effective date of the new rules.

The SEC alleged that the public disclosures by each of these companies downplayed the severity of SolarWinds cyberattack-related intrusions in one or more of the following respects: (i) describing risks as hypothetical (even after these risks had materialized in the SolarWinds incident), (ii) disclosing generic descriptions of cyber risks without disclosing the incident the company experienced, (iii) failing to disclose the nature and extent of data that was accessed in the incident (including the nature of the threat actor and details relating to the data accessed), and (iv) minimizing the impact. The companies paid civil penalties ranging from $990,000 to $4,000,000 to settle the charges.

What this means to you

These cases continue a trend towards aggressive SEC enforcement of public companies' disclosure obligations—particularly as they relate to cybersecurity incidents. The actions highlight the importance of ensuring that disclosures—including cybersecurity incident disclosures under new Item 1.05 of Form 8-K—are accurate and fully reflect all (even arguably) material details. Importantly, none of the companies charged by the SEC failed to make disclosures to the public—rather, the SEC determined that the substance of the disclosures made were not sufficient.

It also should be noted, however, that SEC commissioners Hester M. Peirce and Mark T. Uyeda dissented from these actions, arguing the SEC had engaged in a "hindsight" review to second-guess these companies' materiality determinations while citing immaterial, undisclosed details to support its charges. Their dissent pointed to the SEC's observation in adopting its 2023 Cybersecurity Rule that "immaterial disclosure about cybersecurity incidents may 'divert investor attention' and result in 'mispricing of securities'" and expressed concern that these actions amount to supplemental "regulation by enforcement" which could inadvertently encourage disclosure of excessive immaterial details, undermining the rationale behind the 2023 rule and the addition of Item 1.05 to Form 8-K.

In light of this dissent, and in connection with the expected new incoming SEC administration, we will continue to monitor the SEC's evolving approach to enforcement of its cybersecurity incident disclosure requirements.

Notwithstanding the misgivings expressed by the two dissenting commissioners, however, public companies should bear in mind the following considerations:

Companies should review and update their risk factor disclosures related to cybersecurity incidents, making sure not to disclose a risk as hypothetical after the risk in question has already occurred or to use generic terms when describing specific, known risks.

Companies should review and update their existing cybersecurity-related disclosures—including both substantive disclosures and risk factors—after the company has experienced a material cybersecurity incident.

Companies should review existing disclosure controls and procedures to assess whether current controls are sufficient to make timely determinations of materiality and to report cybersecurity-related information accurately and comprehensively.

Companies should accurately (and fully) describe any material cybersecurity incidents the company experiences in their Form 8-K Item 1.05 disclosures, as well as their ongoing periodic reports.

Contact us

Husch Blackwell's Securities & Corporate Governance team will continue to monitor these developments and their implications. Should you have any questions, including but not limited to what, if anything, you should disclose, please do not hesitate to contact Craig Adoor, Steve Barrett, Robert Joseph, Victoria Sitz, Andrew Spector, Annorah Harris, or your Husch Blackwell attorney.