July 26, 2023

SEC Finalizes Sweeping New Cybersecurity Disclosure Rules for Public Companies

After receiving extensive comments from industry actors and others, the U.S. Securities and Exchange Commission (the "SEC") has now finalized wide-ranging cybersecurity-related disclosure rules first proposed last year. The final rules will require registrants to disclose on the new Item 1.05 of Form 8-K any cybersecurity incident within four business days after the registrant determines the incident to be material. Registrants will also be required to disclose in their annual report on Form 10-K, pursuant to the new Regulation S-K Item 106, their processes for assessing, identifying, and managing material risks from cybersecurity threats, the material impacts of cybersecurity threats and previous cybersecurity incidents, the board's oversight of risks posed by cybersecurity threats, and management's role and expertise in assessing and managing material risks posed by cybersecurity threats.

Disclosures on Form 8-K and Form 6-K will be due beginning the later of 90 days after the date of publication of the new rules in the Federal Register or December 18, 2023. Disclosures on Form 10-K and Form 20-F will be due beginning with annual reports for fiscal years ending on or after December 15, 2023.

While the new rules significantly broaden national standards for cyber-related disclosures, they include several key modifications from the proposed rules:

Scope of 8-K and Periodic Report Disclosures: The new Item 1.05 of Form 8-K has been revised to focus the disclosure primarily on the impacts of a material cybersecurity incident, rather than on details regarding the incident itself. As a result, registrants will *not* be required to disclose the incident's remediation status, whether data has been compromised, or potential system vulnerabilities in such detail that would impede the registrant's response or remediation of the incident.

In addition, updated incident disclosures will be made on a Form 8-K amendment instead of the registrant's periodic reports as initially proposed. The final rule also eliminates proposed Item 106(d)(2) of Regulation S-K, which would have required registrants to make disclosures in their periodic reports when a series of previously undisclosed individually immaterial cybersecurity incidents became material in the aggregate. And disclosures concerning board oversight and governance processes have been streamlined to eliminate more granular disclosures such as the frequency of board discussions of cybersecurity.

Timing of 8-K Disclosures: The SEC adopted a provision authorizing delay in cases where disclosure poses a substantial risk to national security or public safety.

A registrant may delay making a Form 8-K filing if the Attorney General determines that the disclosure poses a substantial risk to national security or public safety and notifies the SEC in writing. Such delay may be for up to 30 days following the date when the disclosure was otherwise required and may be further extended if the AG determines that disclosure continues to pose a substantial risk to national security or public safety. The Department of Justice will notify the affected registrant that communication to the SEC has been made, so that the registrant may delay filing its Form 8-K.

Determination of Materiality: The final rules relieve pressure on registrants to make materiality determinations by requiring such determinations "without unreasonable delay" as opposed to "as soon as reasonably practicable," as originally proposed.

Board Expertise: The proposed requirement to disclose the cybersecurity expertise of board members has been eliminated, with the SEC noting that registrants may provide such information, if relevant, elsewhere in their cybersecurity governance disclosures.

Foreign Private Issuers: The final rule includes parallel requirements for filings by foreign private issuers on Forms 6-K and 20-F.

* * *

Cybersecurity disclosure continues to be a high-priority area for the SEC, including in the agency's enforcement program. The new rules impose expanded and more precise disclosure obligations relative to those currently in effect. Public companies should carefully scrutinize their current cybersecurity-related policies and procedures (including preparedness measures) to identify and address any notable gaps between existing approaches and the new SEC standards.

John F. Savarese
Wayne M. Carlin
Sarah K. Eddy
David M. Adlerstein
Carmen X. W. Lu