KAUFMAN | DOLOWICH

Pending Obligations Under SEC's Cybersecurity Disclosure Rules by Avery Dial , Esq, 11-21-2023

With year-end deadlines fast approaching, public companies should already be preparing for new reporting obligations under the U. S. Securities and Exchange Commission's recently adopted cybersecurity disclosure rules. Starting December 18, most public companies (with the exception of smaller reporting companies) must begin disclosing material aspects of cybersecurity incidents. Certain other provisions pertaining to cybersecurity risk management already went into effect September 5.

The rules, adopted by the SEC this past July, are intended to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and cybersecurity incidents by public companies subject to the reporting requirements of the Securities Exchange Act of 1934 including foreign private issuers. They came in response to several factors including "a substantial rise in the prevalence of cybersecurity incidents" propelled by such factors as "the increase in remote work spurred by the pandemic; the increasing reliance on third-party service provides for information technology services; and the rapid monetization of cyberattacks facilitated by ransomware, black markets for stolen data, and crypto-asset technology," according to the SEC.

The final rules are intended to provide greater transparency for shareholders. In particular, the rules require disclosure about "material cybersecurity incidents" and "periodic disclosures about a registrant's processes to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks," according to rule's language.

What is a Material Cybersecurity Incident

According to the SEC, information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the total mix of information made available." According to the rule, the definition of "cybersecurity incident" extends to "a series of related unauthorized occurrences."

New SEC Disclosure Requirements

The rules will require registrants to disclose on the new Item 1.05 of Form 8-K any cybersecurity incident they determine to be material and to describe the material aspects of the incident's nature, scope, and timing, as well as its material impact or reasonably likely material impact on the registrant, according to the SEC. An Item 1.05 Form 8-K would need to be filed within four business days after a company determines that a cybersecurity incident is material. The disclosure may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing, according to the SEC.

The final rules also add Regulation S-K Item 106, which will require registrants to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents. Item 106 will also require registrants to describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats, according to the SEC. These disclosures will be required in a registrant's annual report on Form 10-K. The rules require comparable disclosures by foreign private issuers on Form 6-K for material cybersecurity incidents and on Form 20-F for cybersecurity risk management, strategy, and governance.

Key Disclosure Deadlines

The Form 10-K and Form 20-F disclosures will be due beginning with annual reports for fiscal years ending on or after December 15, 2023. The Form 8-K and Form 6-K disclosures will be due beginning the later of 90 days after the date of publication in the Federal Register or December 18, 2023. Smaller reporting companies have until June 15, 2024-an additional 180 days before they must begin providing the Form 8-K disclosure. With respect to compliance with the structured data requirements, all registrants must tag disclosures required under the final rules in Inline XBRL beginning one year after initial compliance with the related disclosure requirement, according to the SEC.

How Companies Can Be Proactive

- Establish a process/guidelines to determine what is a material cybersecurity incident within the company.
- Review your company's cyber incident reporting procedures to ensure timely disclosure within the four-business day reporting requirement and update notification procedures as necessary.
- Update company policies and procedures regarding incident response.
- Ensure your company has a comprehensive cybersecurity risk management program in place.
- Identify hierarchy and structure regarding who is in charge for providing oversight of cybersecurity management and response.
- Create a culture of cybersecurity awareness that encourages employees to report potential threats and incidents in a timely manner.

Kaufman Dolowich Can Assist

Public companies need to ensure they are able to navigate and comply with these new cybersecurity incident reporting requirements given the likelihood of increased litigation and greater scrutiny by enforcement officials. Kaufman Dolowich's team of data privacy and cybersecurity attorneys can assist with risk management, compliance, and data breach response including updating company policy and procedures, reviewing cybersecurity risk management programs, evaluating incident response plans, and helping clients comply with post-breach collection, notification, and other procedural requirements imposed by data and cybersecurity regulations.