FACT SHEET

Public Company Cybersecurity Disclosures; Final Rules

The Securities and Exchange Commission adopted final rules requiring disclosure of material cybersecurity incidents on Form 8-K and periodic disclosure of a registrant's cybersecurity risk management, strategy, and governance in annual reports.

Background

In March 2022, the Commission proposed new rules, rule amendments, and form amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and material cybersecurity incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. The Commission observed that cybersecurity threats and incidents pose an ongoing and escalating risk to public companies, investors, and market participants. It noted that cybersecurity risks have increased alongside the digitalization of registrants' operations, the growth of remote work, the ability of criminals to monetize cybersecurity incidents, the use of digital payments, and the increasing reliance on third party service providers for information technology services, including cloud computing technology. The Commission also observed that the cost to companies and their investors of cybersecurity incidents is rising and doing so at an increasing rate. All of these trends underscored the need for improved disclosure.

The proposal followed on interpretive guidance issued by Commission staff in 2011 and by the Commission in 2018 on the application of existing disclosure requirements to cybersecurity risk and incidents. Although registrants' disclosures of material cybersecurity incidents and cybersecurity risk management and governance have improved since the 2011 and 2018 guidance, disclosure practices are inconsistent, necessitating new rules. The proposal was intended to result in consistent, comparable, and decision-useful disclosures that would allow investors to evaluate registrants' exposure to material cybersecurity risks and incidents as well as registrants' ability to manage and mitigate those risks.

What's Required

New Form 8-K Item 1.05 will require registrants to disclose any cybersecurity incident they determine to be material and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the registrant, including its financial condition and results of operations.

Registrants must determine the materiality of an incident without unreasonable delay following discovery and, if the incident is determined material, file an Item 1.05 Form 8-K generally within four business days of such determination. 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. If the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through possible exemptive orders.

New Regulation S-K Item 106 will require registrants to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant. 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.

Form 6-K will be amended to require foreign private issuers to furnish information on material cybersecurity incidents that they make or are required to make public or otherwise disclose in a foreign jurisdiction to any stock exchange or to security holders. Form 20-F will be amended to require that foreign private issuers make periodic disclosure comparable to that required in new Regulation S-K Item 106.

What's Next

The final rules will become effective 30 days following publication of the adopting release in the Federal Register. With respect to Regulation S-K Item 106 and the comparable requirements in Form 20-F, all registrants must provide such disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. With respect to compliance with the incident disclosure requirements in Form 8-K Item 1.05 and in Form 6-K, all registrants other than smaller reporting companies must begin complying on the later of 90 days after the date of publication in the Federal Register or December 18, 2023. Smaller reporting companies will have an additional 180 days and must begin complying with Form 8-K Item 1.05 on the later of 270 days from the effective date of the rules or June 15, 2024. 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.