VORYS

Publications

SEC Adopts Rules on Cybersecurity Management And Disclosure

Related Attorneys

Adam K. Brandt

Roger E. Lautzenhiser, Jr.

Adam L. Miller

Chadwick P. Reynolds

Kimberly J. Schaefer

Brian P. Baxter

Sima E. Zoghbi

Related Services

Corporate and Business Organizations

Securities Law Compliance

CLIENT ALERT | 7.31.2023

On July 26, 2023, the Securities and Exchange Commission (SEC) adopted rules requiring that publicly traded companies disclose material cybersecurity incidents and annually provide material information regarding cybersecurity risk management, strategy, and governance.

The new rules require that registrants disclose on new Item 1.05 of Form 8-K any cybersecurity incident they determine to be material and to describe such incident's nature, scope, and timing, as well as its impact on the registrant. Any applicable Form 8-K will generally be due four business days after a registrant determines that a cybersecurity incident is material (rather than the date of discovery of the incident itself), unless the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety. An instruction to Form 8-K provides that materiality determinations must be made "without unreasonable delay" after discovery of a cybersecurity incident, and the SEC states in the adopting release that "adhering to normal internal practices and disclosure controls and procedures will suffice to demonstrate good faith compliance." The SEC also explains in the adopting release that the analysis for materiality of cybersecurity incidents is the same as the materiality analysis for other securities laws purposes, and that the analysis should take into account qualitative and quantitative factors.

The new rules also add Regulation S-K Item 106, which requires that registrants describe in their annual report on Form 10-K their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects of risks from cybersecurity threats and previous cybersecurity incidents. Item 106 also requires that registrants 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. Notably, the SEC did not adopt the proposed rule that would have required registrants to disclose the cybersecurity expertise, if any, of their respective board members.

The final rules become effective 30 days following publication of the adopting release in the Federal Register. The Form 10-K disclosures must be included beginning with annual reports for fiscal years ending on or after December 15, 2023. The Form 8-K disclosures will be required beginning 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 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.

For additional information on the new rules, see the press release announcing adoption of the final rules and the fact sheet published by the SEC.

Please contact your Vorys attorney with any questions about these rules.