Capital Markets Alert

August 2023

SEC Adopts Cybersecurity Disclosure Rules

The Securities and Exchange Commission (SEC) has adopted explicit rules regarding reporting companies' exposure to cybersecurity risks and risk management, replacing earlier guidance that such risks may be required to be disclosed under the general materiality standard.

In annual reports and Securities Act registration statements, an issuer will be required to describe the company's processes for identifying and managing material cybersecurity risks "in sufficient detail for a reasonable investor to understand those processes." Disclosure should include:

- Whether and how any such processes have been integrated into the company's overall risk management system;
- Whether the registrant engages assessors, consultants, auditors or other third parties in connection with any such processes; and
- Whether the registrant has processes to identify such risks arising from its third-party service providers.

A reporting company also must describe how any cybersecurity risks may have or past incidents have had a material effect on the company, its business strategy, results of operations or financial condition.

An issuer must describe the board of directors' oversight of cybersecurity risks and any board committee responsible for such oversight as well as the processes by which the board or committee is informed about such risks or cybersecurity incidents.

In addition, disclosure is required of management's role in assessing and managing these risks, addressing, among other things:

- Responsible management and the relevant expertise of such persons;
- The processes by which such persons are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
- Whether such persons or committees report information about such risks to the board of directors.

Under a new item—1.05, Material Cybersecurity Incidents—an issuer must report on Form 8-K , any cybersecurity incident that it determines material, within four days of the determination, describing the nature, scope, and timing of the incident and the material impact or reasonably likely material impact on the company, including its financial condition and results of operations. The report must be amended for any updates. Failure to file pursuant to this requirement does not deprive an issuer of the use of Form S-3. Disclosure of cybersecurity incidents must be reported on Form 6-K if the issuer is a foreign private issuer and is required to report it publicly under the laws of its domicile or a foreign securities exchange.

Attorney Advertising

The rules become effective Sept. 5 and apply to annual reports for years ending Dec. 31, 2023, and to current reports beginning Dec. 18, 2023, or June 15, 2024, for smaller reporting companies.

Related Professionals

Norwood P. Beveridge . . . . . nbeveridge@loeb.com
Joan S. Guilfoyle . . . . . jguilfoyle@loeb.com
David C. Fischer . . . . . dfischer@loeb.com

7407 REV1 08-16-2023