LUSE GORMAN
attorneys

August 7, 2023

LEGAL UPDATES AND NEWS

SEC Adopts Disclosure Rules on Cybersecurity Incidents, Risk Management, Strategy, and Governance

On July 26, 2023, the U.S. Securities and Exchange Commission (the "SEC") adopted a final rule requiring public companies to disclose material cybersecurity incidents as they occur and to report on an annual basis material information regarding cybersecurity risk management, strategy, and governance.

What is a Material Cybersecurity Incident?

The definition of "cybersecurity incident" is to be construed broadly and includes "a series of related unauthorized occurrences," and therefore could be triggered by a series of related events that in the aggregate are deemed material. Information is defined as "material" if there is a substantial likelihood that a reasonable shareholder would consider it important in an investment decision.

After the discovery of a cybersecurity incident, determination of materiality must be made without unreasonable delay and adhere to normal internal practices and disclosure controls and procedures to demonstrate good faith compliance. Issuers need to consider whether:

- the incident violated the company's security policies and procedures;
- the incident jeopardized the confidentiality, integrity, or availability of information;
- the incident disrupted, damaged, or caused a loss of operational technology; and/or
- an unauthorized party has accessed, altered, stolen, or threatened to disclose, personally identifiable information or sensitive business information.

New Item 1.05 on Form 8-K

Within four business days from the date an issuer determines that a cybersecurity incident is "material," rather than the date of discovery of the incident itself, disclosure on Form 8-K under Item 1.05 is required. Delayed disclosure, for a period up to 30 days, is permitted in limited circumstances that pose a substantial risk to national security or public safety, as determined by the U.S. Attorney General. However, a failure to timely file Item 1.05 on Form 8-K will not disqualify an issuer from its use of the short form registration statement on Form S-3.

Required Disclosures

In the event there is a material cybersecurity incident, a company must describe:

- the material aspects of the nature, scope and timing of the incident;
- the material impact or reasonably likely material impact on the company, including its financial condition and results of operations; and

- if material information is not determinable or available at the time of filing, the company must note such missing information and file an amendment to the Form 8-K within four days of such missing information becoming determinable or available.

Companies do not need to disclose specific or technical information about the company's planned response to an incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail that would impede the company's response or remediation of the incident.

New Item 106 under Regulation S-K on Form 10-K

Risk Management and Strategy Disclosures

Companies must describe their processes, if any, in sufficient detail for a reasonable investor to understand the assessment, identification, and management of material risks from cybersecurity threats, by addressing:

- whether and how the described cybersecurity processes have been integrated into the company's overall risk management system or processes;
- whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes;
- whether the company has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider; and
- 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 company, including its business strategy, results of operations, or financial condition and if so, how.

Governance Disclosures

Regarding the **board of directors' oversight** of cybersecurity threats, a company must describe:

- the board's oversight of risks from cybersecurity threats, and if applicable, identify any committee's or subcommittee's responsibility for such oversight; and
- management's role in assessing and managing material risks from cybersecurity threats.

Regarding **management's role** of assessing and managing cybersecurity threats, a company must describe:

- whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
- the processes by which such persons or committees 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 or a committee or subcommittee of the board of directors.

Formatting

Cybersecurity disclosures must be tagged using Inline XBRL.

Compliance Dates

Form	Compliance Dates
10-K	• Fiscal years ending on or after December 15, 2023.
8-K	• The later of 90 days after the date of publication in the Federal Register or December 18, 2023. • However, *smaller reporting companies* will have until the later of 270 days after the date of publication in the Federal Register or June 15, 2024.

* * * * *

Please contact any of our attorneys if you have questions regarding the information contained in this newsletter. To learn more about our firm and services, please visit our website.

© 2023 Luse Gorman, PC. Luse Gorman, PC is a Washington, DC-based law firm that specializes in representing domestic and foreign financial institutions in the United States. The information provided herein does not constitute legal advice and relates only to matters of federal law and not to any particular state law.