SEC ADOPTS RULES FOR CYBERSECURITY RISK MANAGEMENT, STRATEGY, GOVERNANCE AND INCIDENT DISCLOSURE

By Brian V. Breheny, Raquel Fox, Marc S. Gerber, William Ridgway and David A. Simon

Brian Breheny, Raquel Fox, Marc Gerber and David Simon are partners in the Washington, D.C. office of Skadden, Arps, Slate, Meagher & Flom LLP. William Ridgway is a partner in Skadden Arps' Chicago office. Contact:
brian.breheny@skadden.com or
raquel.fox@skadden.com or
marc.gerber@skadden.com or
william.ridgway@skadden.com or
david.simon@skadden.com.

On July 26, 2023, the U.S. Securities and Exchange Commission ("SEC") voted 3-2 to adopt final rules[1] that are intended to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934 (including foreign private issuers). Specifically, the SEC's amendments require:

- Current reporting of material cybersecurity incidents.
- Annual reporting of company processes for identifying, assessing and managing material risks from cybersecurity threats; management's role in assessing and managing the company's material cybersecurity risks; and the board's oversight of cybersecurity risks.

Key Requirements of Cybersecurity Incident Disclosure Rules

Form 8-K Trigger

The final rules amend Form 8-K to add new Item 1.05, which requires disclosure within four business days after a company determines that a "cybersecurity incident" experienced by the company is material. The trigger for Item 1.05 of Form 8-K is the date on which the company determines that a cybersecurity incident it has experienced is material, rather than the date of discovery of the incident itself. 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."

Materiality

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 in assessing materiality.

Required Disclosure

In the event disclosure is triggered, 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.
- An instruction to Form 8-K clarifies that companies do not need to disclose specific or technical information about the company's planned response to the incident or its cybersecurity systems in such detail as would impede the company's response or remediation of the incident.

The SEC did not adopt the proposed rule that would have required companies to disclose in their periodic reports any material changes, additions or updates to a prior disclosure under Item 1.05 of Form 8-K or any individually immaterial cybersecurity incidents not previously disclosed that become material in the

aggregate. The adopting release highlighted, however, that the definition of "cybersecurity incident" is intended to be construed broadly and includes "a series of related unauthorized occurrences." As a result, it is possible that Item 1.05 could be triggered by a series of related occurrences that are deemed material in the aggregate.

Delay Due to Risks to National Security or Public Safety

A company may delay disclosure of a material cybersecurity incident for up to 30 days if the U.S. Attorney General determines that disclosure poses a substantial risk to national security or public safety. The disclosure may be delayed for an additional period of up to 30 days if the Attorney General determines that disclosure continues to pose a substantial risk. In extraordinary circumstances, in the case of risk to national security, disclosure may be delayed for a final additional period of up to 60 days. It remains to be seen what processes the U.S. Department of Justice will establish to consider delayed disclosure.

Companies that are subject to the Federal Communications Commission's ("FCC") notification rule for breaches of customer proprietary network information ("CPNI") may delay making the Form 8-K disclosure up to seven business days following notification to the U.S. Secret Service and the Federal Bureau of Investigation, as specified by the FCC rule.

Updating Disclosure

In the event that information required to be disclosed under Item 1.05 of Form 8-K is not determined or is unavailable at the time of the required filing, companies must note the missing information in the initial disclosure and file an amendment to Form 8-K within four business days after such information is determined or becomes available.

There is no specific requirement to provide updated information concerning a cybersecurity incident, either in a Form 8-K or in a company's periodic reports. The SEC noted in the adopting release, however, that companies may have a duty to correct prior disclosure that they determine was untrue at the time it was made or a duty to update disclosure that becomes materially inaccurate after it was made.

Cybersecurity Risk Management, Strategy and Governance Disclosure

Risk Management

New Item 106(b) of Regulation S-K requires a description of the company's processes, if any, for assessing, identifying and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. The rule provides the following nonexclusive list of potential disclosure items:

- Whether and how the described 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 third-party service providers.

In addition, Item 106(b) requires companies to describe 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

New Item 106(c) of Regulation S-K requires companies to disclose information related to the board's and management's roles relating to cybersecurity.

With respect to the board of directors, companies must describe:

- The board's oversight of risks from cybersecurity threats and, if applicable, any board committee or subcommittee responsible for such oversight.
- The processes by which the board or board committee is informed about such risks.

Notably, the SEC did not adopt the proposed rule that would have required companies to disclose the cybersecurity expertise, if any, of the company's board members.

With respect to management, companies must describe management's role in assessing and managing the company's material risks from cybersecurity threats. The rule provides the following nonexclusive list of potential disclosure items:

- 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 is 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.
- Whether such persons or committees report information about such risks to the board of directors or a board committee or subcommittee.

Disclosure by Foreign Private Issuers

Amendments to Forms 20-F establish disclosure requirements for foreign private issuers parallel to those adopted for domestic issuers in Regulation S-K Item 106. Amendments to Form 6-K also parallel those adopted for domestic issuers in Form 8-K Item 1.05, and require foreign private issuers to furnish on Form 6-K information about material cybersecurity incidents that the issuers disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange or to security holders.

Inline XBRL Tagging

The adopted rules require reporting companies to tag disclosure under Item 1.05 of Form 8-K and Item 106 of Regulation S-K using Inline XBRL, with a staggered compliance date of one year beyond initial compliance with the disclosure requirements.

Compliance Dates

- Companies other than smaller reporting companies must begin complying with current reporting of material cybersecurity incidents (on Form 8-K or Form 6-K, as applicable) on the later of 90 days after the date of publication of the final rules 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 reporting of material cybersecurity incidents on the later of 270 days from the effective date of the rules or June 15, 2024.
- Companies must include the cybersecurity risk management, strategy and governance disclosures in their annual reports for fiscal years ending on or after December 15, 2023.
- As noted above, companies will have an additional year after the initial compliance dates for tagging the disclosure using Inline XBRL.

For additional information on the new rules, see the press release announcing adoption of the final rules[2] and the fact sheet published by the SEC.[3]

This article is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice.

Contributing to this article were counsel Andrew J. Brady, Ryan J. Adams and Caroline S. Kim, and associates Leo W. Chomiak, Jeongu Gim, Nicholas D. Lamparski and Joshua Shainess, all of whom are based in the Washington, D.C. office of Skadden, Arps, Slate,

Meagher & Flom. Also contributing: Khadija Messina, an associate in Skadden Arps' Chicago office, and James Rapp, a counsel in Skadden Arps' New York office.

ENDNOTES:

[1]*See* https://www.skadden.com/-/media/files/publications/2023/07/sec-adopts-rules-for-cybersecurity-risk-management/final-rules.pdf.

[2] https://www.sec.gov/news/press-release/2023-139.

[3] https://www.skadden.com/-/media/files/publications/2023/07/sec-adopts-rules-for-cybersecurity-risk-management/fact-sheet-published-by-the-sec.pdf.