SEC Adopts Final Rules on Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure by Public Companies

By **Jesse Michael Brush**, **Garrett A. DeVries**, **Natasha G. Kohne**, **Michelle A. Reed**, **Rosa A. Testani**, **Andrew P. McDonough** and **Patricia M. Precel**

August 3, 2023

On July 26, 2023, the U.S. Securities and Exchange Commission (SEC) adopted **final rules** that generally require public companies to disclose (i) material cybersecurity incidents within four business days after determining the incident was material and (ii) material information regarding their cybersecurity risk management, strategy and governance on an annual basis. The SEC initially issued proposed rules to enhance and standardize disclosures regarding cybersecurity governance and incident reporting by public companies in March 2022. The final rules made some important modifications to the disclosure requirements, which are discussed more fully below and are set forth in **Release No. 33-11216**, but will still require public companies (other than foreign private issuers (FPIs)) to meet substantial compliance obligations, including to:

- Disclose in a current report on Form 8-K information regarding a material cybersecurity incident within four business days after determining the incident was material.
- Amend a prior Form 8-K disclosing a cybersecurity incident to disclose any required information that was not determined or was unavailable at the time of the initial Form 8-K.
- Include in an annual report on Form 10-K a description of processes, if any, for the assessment, identification and management of material risks from cybersecurity threats, and an assessment of cybersecurity risks that are reasonably likely to affect business strategy, results of operations or financial condition.
- Describe in an annual report on Form 10-K 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.
- Tag the cybersecurity disclosures in Inline eXtensible Business Reporting Language (XBRL).

The final rules will also require FPIs to:

- Promptly furnish in a report on Form 6-K information regarding a material cybersecurity incident if otherwise disclosed or required to be disclosed.
- Include in an annual report on Form 20-F updated disclosure regarding incidents previously disclosed on Form 6-K.
- Include in an annual report on Form 20-F a description of processes, if any, for the assessment, identification and management of material risks from cybersecurity threats, and an assessment of cybersecurity risks that are reasonably likely to affect business strategy, results of operations or financial condition.
- Describe in an annual report on Form 20-F 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.
- Tag the cybersecurity disclosures in Inline XBRL.

This Alert summarizes the key takeaways for affected companies and offers recommendations on how to prepare for the new requirements.

Summary of Final Rules

Cybersecurity Incident Disclosure Requirement in a Form 8-K or Form 6-K

Form 8-K

Public companies (other than FPIs) must disclose the following information within four business days of determining that it experienced a material cybersecurity incident:

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

These requirements represent a narrowing of the scope of disclosure originally proposed.[1] The final rules do not require a public company to disclose information regarding cybersecurity incident remediation status, and note that the public company "need not disclose specific or technical information about its planned response to the incident."

There is one narrow exception to disclosure for national security. The final rules permit a limited delay for disclosures where the U.S. Attorney General determines that such disclosure would pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing. Following such determination, a company can delay disclosure for up to 30 days after the date when disclosure was otherwise required. Disclosure can be delayed for up to an additional 90 days upon additional determinations of substantial risk to national security by the Attorney General.

While disclosures are not triggered by the discovery of an incident, a company should avoid delays in making a determination about materiality in order to avoid a disclosure obligation. Instruction 1 to Item 1.05 of Form 8-K requires public companies to make the materiality determination "without unreasonable delay" after discovery of the incident.

Although the final rules eliminated the originally proposed aggregation of immaterial incidents in the periodic disclosure, they did include the concept of aggregation of related cyber intrusions. In the release, the SEC emphasizes that the term "cybersecurity incident" must be construed broadly and extends to "a series of related unauthorized occurrences." Accordingly, this Form 8-K requirement may in some instances be triggered by a series of multiple related intrusions each of which is deemed to be immaterial but which, viewed together, are reasonably likely to have a material impact on the company. The SEC noted that the "related" incident could be repeated attacks by the same threat actor or attacks by different threat actors exploiting the same vulnerability.

Key Point – Impact of Ongoing Investigations

The final Form 8-K disclosure rule does not provide for a reporting delay when there is an ongoing internal or external investigation related to the cybersecurity incident. While the SEC recognized that a delay in reporting could help facilitate law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident and preventing future cybersecurity incidents, the SEC's view is that the importance of timely disclosure of cybersecurity incidents for investors justifies not providing for a reporting delay. Nonetheless, in the final release, the SEC recognizes "that a materiality determination necessitates an informed and deliberative process." Accordingly, while a public company that experiences a cybersecurity incident need not rush to make a premature determination on materiality, the SEC cautioned that the materiality determination "cannot be unreasonably delayed in an effort to avoid timely disclosure."

Form 6-K

FPIs must promptly furnish in a report on Form 6-K information regarding a material cybersecurity incident that such FPI discloses, or is required to disclose, in a foreign jurisdiction, to any stock exchange or to security holders.

Updates on Previously Reported Cybersecurity Incidents Required in Amended Form 8-K or Form 20-F

The final rules require public companies (other than FPIs) to amend a prior current report on Form 8-K disclosing a cybersecurity incident by filing an amendment to the Form 8-K to disclose any required information that was not determined or was unavailable at the time of the initial Form 8-K filing within four business days after such company, without unreasonable delay, determines such information or within four business days after such information becomes available.[2]

The final rules require FPIs to include in an annual report on Form 20-F updated disclosure regarding incidents previously disclosed on Form 6-K.

New Cybersecurity Governance Disclosure Requirements in Annual Reports on Form 10-K and Form 20-F

Regulation S-K Items 106(b) and (c)

Public companies (other than FPIs) must provide disclosure in the Form 10-K of (i) processes,[3] if any, for assessing, identifying and managing material risks from cybersecurity threats, and (ii) the **board's** oversight of cybersecurity risk and **management's** role in assessing and managing material cybersecurity-related risks.

Under Item 106(b) of Regulation S-K, a public company's disclosure of its cybersecurity processes in the Form 10-K should include:

- Whether and how the described cybersecurity processes have been integrated into such 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.
- Whether any risks from cybersecurity threats 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.

Under Item 106(c) of Regulation S-K, the description of the board's cyber-related oversight should include:

- Whether the entire board, specific board members or a board committee or subcommittee, is responsible for the oversight of cybersecurity risks.
- The processes by which the board is informed about cybersecurity risks.

In describing management's role in assessing and managing material risks from cybersecurity threats, Item 106(c) of Regulation S-K directs public companies to disclose, as applicable:

- 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.

- 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.

Form 20-F

The SEC also amended Form 20-F to include disclosure requirements analogous to the requirements of Items 106(b) and 106(c) of Regulation S-K discussed above.

Inline XBRL

Public companies must comply with structured data requirements by tagging the cybersecurity disclosures in Inline XBRL.

Effective Date

The final rules will become effective 30 days following publication of the adopting release in the *Federal Register*. The Form 10-K and Form 20-F disclosures will be due beginning with annual reports for fiscal years ending on or after December 15, 2023. Public companies (other than smaller reporting companies) must begin complying with the Form 8-K and Form 6-K disclosure requirements 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 the Form 8-K disclosure requirements 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 public companies must tag disclosures required under the final rules in Inline XBRL beginning one year after initial compliance with the related disclosure requirement.

Implementing Policies and Procedures to Address the Final Rules

The final rules' window for disclosure necessitates that companies be efficient in identifying, evaluating and assessing materiality of cybersecurity incidents. Here are a few takeaways that companies should be thinking about now to prepare for these new requirements:

- Evaluate disclosure controls and procedures associated with the timing and reporting of cybersecurity risks and incidents.
- Assess whether your board, as currently composed, has adequate depth of cybersecurity experience in relation to the threat of cybersecurity incidents to your operations and financial condition. Where members of management or committees are responsible for managing cybersecurity risk, you should evaluate the relevant expertise of such person or members. Update your annual director and officer questionnaire to identify cybersecurity-related experience.
- Consider your board and management's current role in overseeing the management of cybersecurity risk and whether any updates should be made to related policies and procedures.
- Identify and monitor the practices of third-party service providers and vendors who maintain investor or client information and are at risk of cyberattack. The final rules require companies to discuss whether the company has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider. Consider whether any practices or procedures need to be formalized or strengthened.
- Continue to actively evaluate cybersecurity programs and consider implementation of additional efforts to further cyber hygiene and prevent cybersecurity incidents, such as adopting incident response plans, conducting tabletop exercises, requiring employee training and mandating, and ensuring fundamental cybersecurity protections such as regular patching, complex passwords and multifactor authentication to gain access to systems.

Our cybersecurity team has significant experience preparing boards and companies for cyber incidents, running table top scenarios, developing risk matrices and advising on cyber governance and risk management. In concert with our public company advisory team and in anticipation of the adoption of these final rules, we have been assisting companies with updating their cyber risk management processes, including their third-party programs, and revising disclosures and policies to comply with these new requirements.

If you have questions about this client alert, please contact any Akin lawyer or advisor below:

Jesse Michael Brush
jbrush@akingump.com
+1 212.872.1046

Garrett A. DeVries
gdevries@akingump.com
+1 214.969.2891

Natasha G. Kohne
nkohne@akingump.com
+1 415.765.9505

Michelle A. Reed
mreed@akingump.com
+1 214.969.2713

Rosa A. Testani
rtestani@akingump.com
+1 212.872.8115

Andrew P. McDonough
amcdonough@akingump.com
+1 212.872.8113

Patricia M. Precel
pprecel@akingump.com
+1 212.872.7440

[1] Under the original proposed rules, Item 106(d)(1) of Regulation S-K would have required a much broader disclosure of the following: (1) any material effect of the incident on the company's operations and financial condition; (2) any potential material future impacts on the company's operations and financial condition; (3) whether the company has remediated or is currently remediating the incident; and (4) any changes in the company's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes.

[2] The proposed rules would have required public companies to disclose any material changes, additions, or updates regarding previously reported cybersecurity incidents in Form 10-Q or Form 10-K for the period in which the change, addition, or update occurred. The SEC did not include this requirement in the final rules.

[3] To address the concern that the proposed rules would require disclosure of "the kinds of operational details that could be weaponized by threat actors," the SEC narrowed the disclosure requirement to "processes" rather than "policies and procedures" for managing material cybersecurity risks as originally proposed.