New SEC Rules on Public Company Cybersecurity Disclosures

August 2023

BARNES & THORNBURG LLP

Background

- On March 9, 2022, the Securities and Exchange Commission (the "SEC") released proposed amendments (the "Proposed Amendments") to improve and streamline disclosure relating to cybersecurity risks and incidents.
- Under the existing regulatory framework, neither Regulation S-K nor Regulation S-X *expressly* requires that cybersecurity risk management procedures, cybersecurity risks or incidents be disclosed.
  - In 2011 and 2018, the SEC issued interpretive guidance that did not create any new disclosure obligations but rather presented the SEC's views on how its existing rules should be interpreted in connection with cybersecurity threats and incidents. The interpretive guidance discussed the impact of cybersecurity risks and incidents on disclosure requirements for risk factors, MD&A, and the financial statements and expanded the SEC's interpretive guidance on cybersecurity policies and controls, most notably those related to cybersecurity escalation procedures and the application of insider trading prohibitions. Further, it addressed the importance of avoiding selective disclosure as well as considering the role of the board of directors in risk oversight.
- On July 26, 2023, the SEC (by a 3-2 vote) adopted the final rules.

Timing

- The rules will be effective September 5, 2023.
- With respect to compliance with Form 8-K, Item 1.05, registrants must begin complying on December 18, 2023.
  - Smaller reporting companies will have an additional 180 days and must begin complying with Form 8-K, Item 1.05 on June 15, 2024.
- Issuers will be required to provide Reg. S-K, Item 106 disclosure beginning with annual reports for fiscal years ending on or after December 15, 2023 (i.e., in the Form 10-K filed in early 2024 for companies with a 12/31 year end).
- All registrants must tag disclosures required under the final rules in Inline XBRL (iXBRL) beginning one year after initial compliance with the related disclosure requirement.

Summary of Amendments

Amendment	Disclosure	Timing
Item 1.05 of Form 8-K	• The material aspects of the nature, scope and timing of the material cybersecurity incident. • The material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations.	Four business days after registrant determines it has experienced a material cybersecurity incident. A registrant may delay filing if the U.S. Attorney General determines immediate disclosure would pose a substantial risk to national security or public safety (and further extended if the Attorney General determines the disclosure poses a continuing risk). The original Form 8-K must be amended to disclose any information that was not determined or unavailable at the time of the initial filing.

Summary of Amendments

Amendment	Disclosure	Timing
Item 106(b)(1) of Regulation S-K	Description of registrant's processes for assessing, identifying and managing material risks for cybersecurity threats.	Disclose in Form 10-K.
Item 106(b)(2) of Regulation S-K	Description of whether any risks from cybersecurity threats have materially affected or reasonably likely to affect the registrant's business strategy, results of operations or financial condition.	Disclose in Form 10-K.

Summary of Amendments

Amendment	Disclosure	Timing
Item 106(c)(1) of Regulation S-K	Describe board's oversight of risks from cybersecurity threats and, if applicable, identify any board committee responsible for such oversight and their process for staying informed of such risks.	Disclose in Form 10-K.
Item 106(c)(2) of Regulation S-K	Describe management's role in assessing and managing material risks from cybersecurity threats.	Disclose in Form 10-K.

Item 1.05 of Form 8-K

- Scope of Disclosure:
  - Companies must disclose the material aspects of the nature, scope and timing of the cybersecurity incident, rather than the originally proposed prescribed list, which included, among other things, remediation status and data compromises.
  - The adopting release highlights that the rule's inclusion of "financial condition and results of operations" is not exclusive, and companies should consider qualitative factors *and* quantitative factors in assessing the material impact of a cybersecurity incident.
  - Companies need not disclose specific or technical information about its planned response, related networks or devices, or system vulnerabilities if the information would impede the company's remediation of the cybersecurity incident.
  - The final rules apply to the material impact of incidents, as well as the reasonably likely material impact on the registrant.

Item 1.05 of Form 8-K

- Timing:
  - Disclosure is required within four business days after determination that a material cybersecurity incident has occurred.
  - The instructions to this item provide that determinations of materiality be made "without unreasonable delay after discovery of the incident," compared to "as soon as reasonably practicable after discovery of the [cybersecurity] incident" per the proposed rules.
  - The untimely filing of an Item 1.05 Form 8-K will not result in the loss of Form S-3 eligibility.
  - As finally adopted, the rules include for a narrow category of cybersecurity incidents a national security exemption permitting delay of filing for up to 120 days if the US Attorney General notifies the SEC that disclosure would result in substantial risk to national security.

Item 1.05 of Form 8-K

- Materiality Assessment:
  - In determining whether a cybersecurity incident is "material," the item applies the existing standard of materiality under the federal securities laws, i.e., something is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available."
- Aggregation
  - Companies must consider the cumulative impact of a "series of related unauthorized occurrences" in connection with their materiality analysis of a cybersecurity incident.
  - Accordingly, when a company finds that it has been materially affected by what may appear as a series of related cyber intrusions, Item 1.05 may be triggered even if the material impact or reasonably likely material impact could be parceled among the multiple intrusions to render each by itself immaterial.

Item 1.05 of Form 8-K

- Safe Harbor from Liability
  - The adopting release amends Rules 13a-11(c) and 15d-11(c) under the Exchange Act to include new Item 1.05 in the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) or Rule 10b-5. The SEC's view is that the safe harbor is appropriate in this context because the triggering event for Item 1.05 disclosures requires management to make a rapid materiality determination.

Item 1.05 of Form 8-K

- Updated Incident Disclosure:
  - The proposed rules would have required periodic updates to Item 1.05 disclosure in quarterly or annual reports.
  - In a departure from the proposed rules, the final rules include an instruction to Item 1.05 of Form 8-K directing the registrant to include in its Item 1.05 Form 8-K a statement identifying any information called for in Item 1.05(a) that is not determined or is unavailable at the time of the required filing and then file an amendment to its Form 8-K containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available.

New Cybersecurity Governance Disclosures in Form 10-K

- New Regulation S-K Item 106(b)(1) requires registrants to describe their "processes, if any, for assessing, identifying and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes."
- In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:
  - Whether and how any such processes have been integrated into the registrant's overall risk management system or processes;
  - Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
  - Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

New Cybersecurity Governance Disclosures in Form 10-K

- New Regulation S-K Item 106(b)(2) requires a registrant 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 registrant, including its business strategy, results of operations, or financial condition and if so, how.
  - With respect to the Item 106(b)(2)'s requirement to describe any risks as a result of any previous cybersecurity incidents, registrants should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.
- Registrants will need to consider how they describe their processes to avoid giving bad actors a "road map" to potential vulnerabilities in them or in associated information systems.

Board Oversight of Risk Disclosures

- Regulation S-K Item 106(c)(1) requires disclosure with respect to *board oversight* of risks from cybersecurity incidents.
  - If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.
  - The Commission declined to include Item 407(j) of Regulation S-K in the final rules, which would have required registrants to disclose the cybersecurity expertise of a board's directors.
  - Also, Item 106(c)(1) will not require details regarding the frequency that the board or a committee discusses cybersecurity risks or whether and how the board considers cybersecurity risks as part of its business strategy, risk management and financial oversight.

Management Disclosures

- Regulation S-K Item 106(c)(2) requires disclosure with respect to management's role in assessing the registrant's material risks from cybersecurity threats.
- In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of 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 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.
- Relevant expertise of management may include, for example: prior work experience in cybersecurity; any relevant degrees or certifications; any knowledge, skills, or other background in cybersecurity.

iXBRL Tagging Required

- The rule requires registrants to tag information provided in response to Item 1.05 of Form 8-K and Item 106 of Regulation S-K in iXBRL.
- iXBRL tagging will have a delayed compliance date of 1 year beyond the initial compliance with the disclosure requirements.

Key Takeaways

- Revisit Incident Response Plans
  - An aggressive reporting regime emphasizes the need for registrants to have an incident response plan and forensic and other experts ready to move quickly in the event of an attack, in order to attempt to quickly determine the information needed to make a disclosure decision.
- Revisit Disclosure Controls and Procedures
  - Assess the efficacy of their disclosure controls and procedures with respect to cybersecurity incidents (including a "series of related unauthorized occurrences") in order to effectively respond to determine the materiality of an incident and therefore the trigger for Form 8-K disclosure.
  - Discuss process within the Disclosure Committee
- Evaluate board and committee oversight of material cybersecurity risks
- Evaluate management's role in assessing and managing material cybersecurity risks
  - Consider expertise of such persons or members with a view toward new disclosure requirements
  - Consider preparing draft disclosure of the actual "processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents."