BARNES & THORNBURG LLP

ALERTS

FAQs On The New SEC Rules On Public Company Cybersecurity Disclosures

August 10, 2023

On July 26, 2023, the Securities and Exchange Commission (SEC) in a 3-to-2 vote, adopted final rules requiring the disclosure of material cybersecurity incidents and cybersecurity risk management, strategy, and governance by public companies, including foreign private issuers. As the rules have now been published in the Federal Register and are set to go effective on September 5, 2023, set forth below are some FAQs on the new rules to help answer some common questions.

1. Does the effective date of September 5, 2023, mean that all disclosures under the new rules are required on and after this date?

While the final rules are effective September 5, 2023, the date for actual disclosure compliance is later and is triggered off the effective date of the rules. With respect to Item 106 of Regulation S–K and Item 16K of Form 20–F, all registrants must provide such disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. With respect to compliance with the incident disclosure requirements in Item 1.05 of Form 8–K and in Form 6–K, all registrants other than smaller reporting companies must begin complying on December 18, 2023. Smaller reporting companies are being given an additional 180 days from the non-smaller reporting company compliance date before they must begin complying with Item 1.05 of Form 8–K, on June 15, 2024.

With respect to compliance with the structured data requirements, all registrants must tag disclosures required under the final rules in Inline XBRL beginning one year after the initial compliance date for any issuer for the related disclosure requirement. Specifically:

RELATED PEOPLE

Jay H. Knight
Partner
Nashville

P 615-621-6009
F 615-621-6099
Jay.Knight@btlaw.com

Taylor K. Wirth
Partner
Nashville

P 615-621-6010
F 615-621-6099
Taylor.Wirth@btlaw.com

RELATED PRACTICE AREAS

Corporate
Securities and Capital Markets

- For Item 106 of Regulation S–K and Item 16K of Form 20–F, all registrants must begin tagging responsive disclosure in Inline XBRL beginning with annual reports for fiscal years ending on or after December 15, 2024; and
- For Item 1.05 of Form 8–K and Form 6–K all registrants must begin tagging responsive disclosure in Inline XBRL beginning on December 18, 2024.

2. Can you provide a summary of the amendments?

Please see below a summary chart of the 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.
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	Disclose in Form 10-K.

	cybersecurity threats have materially affected or are reasonably likely to affect the registrant's business strategy, results of operations or financial condition.	
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.

3. What are the new Item 1.05 of 8-K amendments?

The final rule adds new Item 1.05 to Form 8-K, which requires companies to determine whether a cybersecurity incident is material "without unreasonable delay after discovery of the incident."

Regarding the scope of the 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 their 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.

With respect to the timing of the 8-K disclosure:

- 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 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.

4. How is materiality determined under the new Item 1.05 of Form 8-K?

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." The SEC's adopting release also stated, "Doubts as to the critical nature" of the relevant information should be "resolved in favor of those the statute is designed to protect," namely investors, quoting *TSC Industries, Inc. v. Northway, Inc.*

Moreover, the SEC states,

"The rule's inclusion of "financial condition and results of operations" is not exclusive; companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident. By way of illustration, harm to a company's reputation, customer or vendor relationships, or competitiveness may be examples on a material impact on the company. Similarly, the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and Federal Governmental authorities and non-U.S. authorities, may constitute a reasonably likely material impact on the registrant." (page 29-30)

5. How is aggregation of individually immaterial cybersecurity incidents treated under new Item 1.05?

The definition of "cybersecurity incident" in new Item 1.05 extends to "a series of related unauthorized occurrences." The SEC states that this reflects that cyberattacks sometimes compound over time, rather than present as a discrete event. 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. One example was provided in the SEC's proposing release: the same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material. The SEC provided another example describing a series of related attacks from multiple actors exploiting the same

vulnerability and collectively impeding the company's business materially.

6. Did the SEC provide any liability protection for these new 8-K disclosures?

Yes, 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. Likewise, the SEC amended General Instruction I.A.3.(b) of Form S-3 and General Instruction I.A.2 of Form SF-3 to provide that an untimely filing on Form 8-K regarding new Item 1.05 would not result in loss of Form S-3 or Form SF-3 eligibility.

7. Does Item 1.05 have any updating requirement to report on developments in the cybersecurity incident?

In the SEC's initial proposed rules, it proposed to require updated cybersecurity disclosure in periodic reports. For example, if a registrant previously provided disclosure regarding one or more cybersecurity incidents pursuant to Item 1.05 of Form 8-K, proposed Item 106(d)(1) of Regulation S-K would have required such registrant to disclose "any material changes, additions, or updates" on the registrant's quarterly report on Form 10-Q or annual report on Form 10-K.

However, 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. This change mitigates commenters' concerns with the updating requirement in the proposed rules.

The SEC's adopting release further states, "We appreciate that new information on a reported cybersecurity incident may surface only in pieces; the final rules, however, do not require updated reporting for all new information. Rather, Instruction 2 to Item 1.05 directs companies to file an amended Form 8-K with respect to any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing."

8. What are the exceptions permitting reporting delays to the 8-K?

The SEC introduced two narrow exceptions that allow for a delay in reporting a material cybersecurity incident on Form 8-K.

- Pursuant to Item 1.05(c), a registrant may delay making an Item 1.05 Form 8-K filing if the Attorney General determines that the

disclosure poses a substantial risk to national security or public safety and notifies the SEC of such determination in writing. Initially, disclosure may be delayed for a time period specified by the Attorney General, up to 30 days following the date when the disclosure was otherwise required to be provided. The delay may be extended for an additional period of up to 30 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing. Outside of extraordinary circumstances or an exemptive order issued by the SEC, the maximum delay permitted under this exception will be 60 days.

- The second exception (in paragraph (d) to Item 1.05) is also extraordinarily limited, and applies only to companies subject to the Federal Communications Commission's (FCC's) notification rule for breaches of customer proprietary network information (CPNI). The FCC's rule requires covered entities to notify the United States Secret Service (USSS) and Federal Bureau of Investigation (FBI) no later than seven business days after reasonable determination of a CPNI breach and to refrain from disclosing the breach until seven days have passed following notification to the USSS and FBI. The SEC's final rule permits companies subject to the notification requirements to delay making the Item 1.05 disclosure up to seven business days following notification to the USSS and FBI, with written notification to the SEC.

- Finally, while not an exception built into the final rule, footnote 131 of the adopting release recognizes another built-in exception found in Exchange Act Rule 0-06, which provides for the omission of information that has been classified by an appropriate department or agency of the federal government for the protection of the interest of national defense or foreign policy. If the information a registrant would otherwise disclose on an Item 1.05 Form 8-K or pursuant to Item 106 of Regulation S-K or Item 16K of Form 20-F is classified, the registrant should comply with Exchange Act Rule 0-6.

9. What are the new cybersecurity disclosures for periodic reports?

The final rule introduces new Item 106 of Regulation S-K, which at a high level will require more discussion in Part I of the Form 10-K of the following areas: 1) cybersecurity risk management and strategy, and 2) governance.

Risk Management and Strategy

New Item 106(b)(1) will require a registrant to describe its "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

- Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider

Governance Disclosure

New Item 106(b)(2) will require 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.

Board Oversight of Risk Disclosure

- 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 SEC 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.
    - 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

- 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.

10. What are the iXBRL tagging requirements?

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 one year beyond the initial compliance with the disclosure requirements.

11. What are some key takeaways from the new rule?

Some key takeaways and action items from the new rule are presented below:

- 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 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."

12. Can you share a PowerPoint presentation of the new rules that I could use to educate management and/or board?

Yes, download it here.

For more information, please contact the Barnes & Thornburg attorney with whom you work or Jay Knight at 615-621-6009 or jay.knight@btlaw.com or Taylor Wirth at 615-621-6010 or taylor.wirth@btlaw.com.