SEC Final Rule Summary: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

On July 26, 2023, the U.S. Securities and Exchange Commission voted 3-2 to adopt a final rule applicable to public companies imposing (1) new disclosure requirements around cybersecurity risk management and governance and (2) obligations to timely disclose material cybersecurity incidents. Key provisions of the final rule are summarized below.

Form 10-K Disclosures Regarding Risk Management, Strategy, and Governance

Effective for Annual Reports for Fiscal Years Ending On or After Dec. 15, 2023

- **Cybersecurity Risk Management and Strategy (Item 106(b) of Regulation S-K):** Form 10-K is required to include disclosures regarding the company's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, described in sufficient detail for a reasonable investor to understand those processes.
  - *Disclosures should include:* **(1)** whether and how any such processes have been integrated into the company's overall risk management system or processes; **(2)** whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes; and **(3)** whether the company has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider. The rules indicate that the SEC views this list as non-exhaustive.
  - *Disclosures must:* 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.
    - *Cybersecurity Threat*: defined as any potential unauthorized occurrence on or conducted through a company's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a company's information systems or any information residing therein.
- **Governance (Item 106(c) of Regulation S-K):** Form 10-K must include disclosure regarding the role of the **board** and **management** in cybersecurity governance.
  - *Board:* Describe the board's oversight of risks from cybersecurity threats, including, if applicable, the board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and the process by which the board or relevant committee is informed about such risks.
  - *Management:* Describe management's role in assessing and managing material risks from cybersecurity threats, as well as its role in implementing cybersecurity policies, procedures, and strategies.
    - *Disclosures should include*: **(1)** whether certain management positions or committees are responsible for managing cybersecurity risk and the relevant expertise of such persons; **(2)** the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and **(3)** whether such persons or committees report information about cybersecurity risk to the board or a board committee. The SEC views this list as non-exhaustive.

Form 8-K Disclosure of Material Cybersecurity Incidents

Likely Effective Dec. 18, 2023

- **Current Reporting (Item 1.05 of Form 8-K):** Companies must disclose a **"cybersecurity incident"** on Form 8-K within **four business days** after **determining the incident is material**.
  - *Materiality and Materiality Determinations*: An incident is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision. The materiality determination "must be made without unreasonable delay after discovery of an incident."

- *Cybersecurity Incident*: defined as an unauthorized occurrence, *or a series of related unauthorized occurrences*, on or conducted through a company's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing therein.
- *Information Systems*: defined as electronic information resources, owned or used by the company, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the company's information to maintain or support the company's operations.
- *Timeline:* Disclosure must be made within four business days after the materiality determination, with limited exceptions and omissions including at the request of the Department of Justice and for classified information.
  - *United States Department of Justice Delay*: if the Department of Justice, through the Attorney General, determines that the required disclosure poses a substantial risk to national security or public safety and notifies the SEC of such determination in writing, the company may delay its current report for the time specified by the Attorney General, up to 30 days. Additional delays may be available as determined by the Department of Justice.
- *Limited Safe Harbor*: Failure to file a Form 8-K on a timely basis will not result in a loss of Form S-3 eligibility. In addition, the rules provide a limited safe harbor from securities fraud liability; Rules 13a-11(c) and 15d-11(c) have been amended to provide that failure to file a Form 8-K under the new cybersecurity disclosure requirement will not be a basis for antifraud liability under Rule 10b-5 of the Securities Exchange Act of 1934, as amended.

- **Content of Disclosures:** *Disclosures must include*: **(1)** material aspects of the nature, scope, and timing of the incident; and **(2)** the material impact or reasonably likely material impact on the company, including its financial condition and results of operations.
  - *Disclosures do NOT need to include:* Technical information about a planned response, cybersecurity systems, related networks and devices, or vulnerabilities "in such detail as would impede the company's response or remediation of the incident."
- **Updating Disclosures of Material Cybersecurity Incidents:** If a company makes a disclosure of a material cybersecurity incident, but has not determined or does not have information that is required to be disclosed (such as the nature, scope, timing, and impact of the incident), the company shall include a statement to this effect in the Form 8-K.
  - *Subsequent Disclosure:* In this case, the company must file an amendment to the initial incident disclosure Form 8-K within four business days after the company **(1)** without unreasonable delay, determines such information or **(2)** such information becomes available.

iXBRL Tagging
New Form 8-K and Form 10-K disclosures must be tagged in iXBRL, subject to 1 year phase-in

Enforcement Posture and Privilege Considerations: Even before the adoption of this rule, the SEC has taken an aggressive stance in investigating cybersecurity incidents and related disclosures/disclosure controls. In these investigations, the SEC has made demands for potentially privileged information and documents, including:
- **(1)** inputs and substance of materiality determinations;
- **(2)** "worksheets" or outputs of materiality determinations; and
- **(3)** information and work product from investigations conducted following an incident, even when such investigations occur at the direction of counsel.

Companies can reasonably expect the SEC to continue this pattern of behavior, and that an SEC inquiry will follow either **(1)** the disclosure of a cybersecurity incident, or **(2)** *non-disclosure* of a cybersecurity incident the SEC believes may have impacted the company, such as after a publicly reported incident believed to impact a range of entities. When conducting materiality determinations, companies should confirm processes are in place to protect privilege where appropriate, taking into account anticipated requests from both the SEC and the company's own auditors.