Client Alert

McGONIGLE
A PROFESSIONAL CORPORATION

7 Things You Need to Know About the Proposed SEC Cybersecurity Rules and Amendments for Public Companies

On March 9, 2022, the U.S. Securities and Exchange Commission (the "SEC") issued proposed rules and amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies. This is what you need to know:

1. **The proposed rules require public companies to disclose information about material cybersecurity incidents within four business days**. Proposed Item 1.05 in the Form 8-K would require the following information to be disclosed about material cybersecurity incidents: (i) when the incident was discovered and whether it is ongoing; (ii) a brief description of the nature and scope of the incident; (iii) whether any data was stolen, altered, accessed, or used for any unauthorized purpose; (iv) the effect of the incident on the registrant's operations; and (v) whether the registrant has remediated or is currently remediating the incident. Notably, the trigger for an Item 1.05 Form 8-K disclosure is the date on which a registrant determines that a cybersecurity incident it has experienced is material, rather than the date of discovery of the incident. The SEC clarified that information in this context 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" and provided the following examples of incidents that could be material: accidental exposure of data, theft of sensitive business information, personally identifiable information, or intellectual property, threats to sell or publicly disclose sensitive data, and ransomware. Proposed Item 1.05 would not provide for a reporting delay where there is an ongoing internal or external investigation related to the cybersecurity incident.
2. **The proposed rules mandate ongoing cybersecurity incident reporting disclosure**. Proposed Item 106(d) of Regulation S-K and Proposed Item 16J(d) of Form 20-F require disclosure (i) relating to previously disclosed cybersecurity incidents; and (ii) to the extent known to management, when a series of previously disclosed individually immaterial cybersecurity incidents has become material in the aggregate.
3. **The proposed cybersecurity incident disclosure rules impact foreign private issuers.** The proposed rules would subject foreign private issuers to the same Form 20-F disclosure requirements and would amend the Form 6-K to add "cybersecurity incidents" as a reporting topic.
4. **The proposed rules require enhanced disclosure of public companies' cybersecurity risk management and strategy.** Proposed Item 106(b) of Regulation S-K would require registrants to disclose their policies and procedures relating to identification and management of cybersecurity risks and threats, including operational risk, intellectual property theft, fraud, extortion, harm to employees or customers, violation of privacy laws and other litigation and legal risk, and reputational risk. The proposed rules specifically pinpoint the following items requiring disclosure: (i) cybersecurity risk assessment programs and descriptions of such programs; (ii) the engagement of assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program; (iii) policies and procedures relating to cybersecurity risks posed by third-party vendors; (iv) activities undertaken to prevent, detect, and minimize the effects of cybersecurity incidents; (v) business continuity, contingency, and recovery plans for cybersecurity incidents; (vi) whether previous cybersecurity incidents have informed changes in the registrant's governance, policies and procedures, or technologies; (vii) a description of how cybersecurity-related risks or incidents have affected or are reasonably likely to affect the registrant's results or financial condition; and (vii) a description of how cybersecurity risks are considered as part of the registrant's business strategy, financial planning, and capital allocation.
5. **The proposed rules require disclosure regarding public companies' cybersecurity governance at the board and management levels**. Proposed Item 106(c) of Regulation S-K would require disclosure

of a registrant's cybersecurity governance, including the board's oversight of cybersecurity risk and a description of management's role in assessing and managing cybersecurity risks, the relevant expertise of such management, and its role in implementing the registrant's cybersecurity policies, procedures, and strategies.

6. **The proposed rules mandate disclosure of board member cybersecurity expertise**. Proposed Item 407(j) of Regulation S-K would require disclosure in annual reports and certain proxy filings if any members of the registrant's board have expertise in cybersecurity, including the names of any such directors and any detail necessary to fully describe the nature of the expertise.
7. **The proposed rules contain three safe harbors**. The proposed rules identify the following three safe harbors: (i) an untimely filing on the Form 8-K regarding Proposed Item 1.05 (material cybersecurity incidents) would not result in a loss of eligibility to register securities with the SEC, provided that the Form 8-K reporting is current at the time the securities registration documents are filed; (ii) an untimely filing on the Form 8-K regarding Proposed Item 1.05 is eligible for a limited safe harbor from liability under the Section 10(b) or Rule 10b-5 anti-fraud provisions of the federal securities laws; and (iii) any board member who is determined to have expertise in cybersecurity will not be deemed an expert under the federal securities laws as a result of such designation (*i.e.*, Proposed Item 407(j) would not impose on such person any duties, obligations or liability that are greater than the duties, obligations, and liabilities imposed on such person as a board member, even if they are identified as a cybersecurity expert).

Comments on the proposed rules are due on May 9, 2022 or 30 days after publication in the Federal Register, whichever is later. McGonigle can assist any public company that wishes to submit a comment letter regarding the myriad of issues raised by the proposed rules, including:

- The incident reporting requirement, including the types of incidents that must be reported, the content of the disclosure, whether four business days is a realistic amount of time to report an incident, and whether the reporting requirement may be delayed for any reason.
- Whether disclosure of cybersecurity events actually benefits investors.
- Whether registrants should be able to withhold information about incidents and their cybersecurity program that might be exploited by threat actors.
- Whether public companies should be required to review past unreported and immaterial incidents to determine if, in the aggregate, they meet the materiality threshold for disclosure.
- The requirement to disclose directors with cybersecurity expertise.
- Any other relevant aspect of the proposed rules.

To discuss this matter, please contact the following McGonigle lawyers:

JOSEPH FACCIPONTI
PARTNER
CHIEF PRIVACY OFFICER
(212) 880-3966
jfacciponti@mmlawus.com

SHARON O'SHAUGHNESSY
PARTNER
CHIEF DIVERSITY, EQUITY & INCLUSION OFFICER
(212) 880-3990
soshaughnessy@mmlawus.com