Crowell

# CLIENT ALERT

## SEC Proposes New Cybersecurity Risk and Incident Disclosure Obligations

**March 15, 2022**

On March 9, 2022, the Securities and Exchange Commission (SEC) issued proposed rules and amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies (registrants) that are subject to the reporting requirements of the Securities Exchange Act of 1934.

The stated intent of the proposed amendments is to better inform investors regarding registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents. SEC's position is that "consistent, comparable, and decision-useful disclosures" would allow investors to assess exposure to cybersecurity risks and incidents, including a registrant's ability to manage and mitigate those risks and incidents.

As further summarized below, the requirements added by the SEC's proposal include obligations to disclose information related to a material cybersecurity incident within four business days, as well as heightened requirements for disclosing information relating to cyber-related risk management, strategy, and governance. Importantly, the reporting obligations contained in the SEC's proposal underscore corporate executive leadership's role in and responsibility for overseeing the cybersecurity of their respective companies.

The proposal is consistent with prior signaling from SEC Chair Gary Gensler that changes were coming, as he highlighted, for example, during his January 2022 remarks at Northwestern School of Law's Annual Securities Regulation Institute. The proposal's direction is also consistent with the significant uptick in the SEC's activity concerning cybersecurity-related matters following the SolarWinds supply chain attack, after which the SEC reportedly opened a probe into the attack's effects and companies' disclosures.

In the immediate term, the SEC's proposal shows that this area is still evolving, but it also clearly signals that there is likely to be continuing increased SEC activity in this area. While the evolving nature of the area may for the moment create challenges for the SEC to bring enforcement cases, it also puts public company executives on notice that they are responsible for their companies' cyber-related actions to prepare for and in response to cyber-attacks.

The following is a summary of updates from the SEC's proposal and Fact Sheet, which provides additional context related to the proposed cybersecurity amendments:

**Reporting cybersecurity incidents on Forms 8-K**

- Requiring current reporting about material cybersecurity incidents on Form 8-K within four business days;
- Amending Form 6-K to add "cybersecurity incidents" as a reporting topic;

**Disclosure about cybersecurity incidents in periodic reports**

- A registrant's policies and procedures to identify and manage cybersecurity risks;

- Management's role in implementing cybersecurity policies and procedures;
- Updates about previously reported material cybersecurity incidents;
- Requiring updated disclosures relating to previously disclosed cybersecurity incidents and to require disclosure, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate;

**Disclosure of a registrant's risk management, strategy and governance regarding cybersecurity risks**

- Requiring registrants to provide more consistent and informative disclosure regarding their cybersecurity risk management and strategy;
- Requiring disclosure of whether cybersecurity related risk and previous incidents have affected or are reasonably likely to affect the registrant's results of operations or financial condition;
- Requiring a description of management's role in assessing and managing cybersecurity-related risks and in implementing the registrant's cybersecurity policies, procedures, and strategies;

**Disclosure regarding the board of directors' cybersecurity expertise**

- Requiring disclosure about the cybersecurity expertise of members of the board of directors of the registrant, if any;

**Periodic disclosure by foreign private issuers (FPI)**

- Requiring an FPI to include in its annual report on Form 20-F the same type of disclosure that would be required in periodic reports filed by domestic registrants:

  **- Item 106 of Regulation S-K.** (1) provide updated disclosure in periodic reports about previously reported cybersecurity incidents; (2) describe its policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity risks as part of its business strategy, financial planning and capital allocation; and (3) require disclosure about the board's oversight of cybersecurity risk, management's role in assessing and managing such risk, management's cybersecurity expertise, and management's role in implementing the registrant's cybersecurity policies, procedures, and strategies; and

  **- Item 407 of Regulation S-K.** Requiringdisclosure of whether any member of the registrant's board has expertise in cybersecurity, and if so, the nature of such expertise.

The amendments also require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (Inline XBRL).

***

Crowell & Moring LLP is highly experienced at advising companies that are navigating cybersecurity and SEC compliance issues such as these. We can provide guidance regarding this Alert and assist with privileged investigations, compliance efforts and other related activities.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

**Evan D. Wolff**
Partner – Washington, D.C.
Phone: +1.202.624.2615
Email: ewolff@crowell.com

**Matthew B. Welling**
Partner – Washington, D.C.
Phone: +1.202.624.2588
Email: mwelling@crowell.com

**Daniel L. Zelenko**
Partner – New York
Phone: +1.212.895.4266
Email: dzelenko@crowell.com

**Garylene (Gage) Javier, CIPP/US**
Associate – Washington, D.C.
Phone: +1.202.654.6743
Email: gjavier@crowell.com