Corporate Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Disclosing Cyber Incidents and Risks: SEC Proposes Rules to Enhance and Standardize Cyber Disclosures and Incident Reporting by Public Companies

March 11, 2022

Key Points:

- Proposed amendments bolster cyber disclosure and incident reporting requirements to better inform investors about a company's risk management, strategy and governance relative to cyber issues.
- Under the proposed rules, public companies would be required to:
  - Report a material cybersecurity incident within four business days.
  - Disclose cybersecurity policies and procedures for identifying and managing cyber risks.
  - Provide updates on any material changes to reported cybersecurity incidents.
  - Present cybersecurity disclosures in Inline XBRL to make them more readily available and easily accessible.
- This Alert summarizes the key takeaways for affected companies and offers recommendations on how to prepare for the potential new requirements.

The U.S. Securities and Exchange Commission (SEC) in a 3-1[1] vote on Wednesday, March 9, 2022, proposed amendments to enhance and standardize disclosures regarding cybersecurity governance and incident reporting by public companies. Such amendments are intended to better inform investors about a company's risk management, strategy and governance relative to cyber issues and to provide timely notification of material cybersecurity incidents. They would require a company to:

- disclose in a Form 8-K or Form 6-K, as applicable, information regarding a material cybersecurity incident within four business days after determining the incident was material;
- disclose in its Form 10-K or Form 20-F, as applicable, policies and procedures related to, and governance over, cybersecurity;

Contact Information

If you have any questions concerning this alert, please contact:

Cynthia Perez Angell
Senior Practice Attorney
cangell@akingump.com
San Antonio
+1 713.250.2245

Peter I. Altman
Partner
paltman@akingump.com
Los Angeles
+1 310.728.3085

Garrett A. DeVries
Partner
gdevries@akingump.com
Dallas
+1 214.969.2891

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Cynthia M. Mabry
Partner
cmabry@akingump.com
Houston
+1 713.220.8130

Ian P. McGinley
Partner
imcginley@akingump.com
New York
+1 212.872.1047

- disclose in its Forms 10-Q and 10-K or Form 20-F, as applicable, updates on previously reported cybersecurity incidents;
- disclose in its proxy statement any cybersecurity expertise of its board; and
- present cybersecurity disclosures in Inline XBRL.

The SEC is seeking comments by the 30th day after publication in the Federal Register or May 9, 2022, whichever is later.

Background

In 2011, the Division of Corporation Finance issued interpretive guidance on companies' disclosure obligations relating to cybersecurity risks and incidents, noting that such items should be addressed in their risk factors and Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A), if applicable. In 2018, the SEC issued additional interpretive guidance that urged companies to consider the materiality of cybersecurity risks and incidents when preparing and evaluating their filing disclosure and reminded companies of: (i) the importance of adopting cybersecurity policies and procedures, and (ii) the application of insider trading prohibitions in the cybersecurity context.

The proposed rules build on such guidance and, as noted in SEC Chair Gary Gensler's statement, are the third rulemaking project that the SEC has proposed recently involving cybersecurity and follow a line of enforcement proceedings that reflect the SEC's increased scrutiny of companies' cybersecurity practices and disclosures (which we discussed in greater detail here). Previously, on January 27, 2022, the SEC voted to propose expanding Regulation Systems Compliance and Integrity (SCI) to certain government securities trading platforms. Then, on February 9, 2022, the SEC voted to propose new obligations for registered investment advisers, registered investment companies, and business development companies with respect to cybersecurity. As of the date of this alert, the comment periods for both proposals remain open.

Summary of Proposed Amendments

Form 8-K

Disclose the following information within four business days of determining that it experienced a material cybersecurity incident:

- when the incident was discovered and whether it is ongoing;
- a brief description of the nature and scope of the incident;
- whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
- the effect of the incident on the company's operations; and
- whether the company has remediated or is currently remediating the incident.

The SEC provided a non-exclusive list of examples of incidents that could trigger disclosure in the proposing release if deemed material. These included, among others, "[a]n unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset (data, system, or network); or violated the [company's] security policies or procedures"[2] and "[a]n incident in which an

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Paul V. Monsour
Counsel
pmonsour@akingump.com
Houston
+1 713.250.2142

unauthorized party accessed, or a party exceeded authorized access, and altered, or has stolen sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the [company]."[3]

While disclosures are not triggered by the discovery of an incident, a company should avoid delays in making a determination about materiality in order to avoid a disclosure obligation. Instruction 1 to proposed Item 1.05 states: "a [company] shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."

Key Point - Impact of Ongoing Investigations
The proposed Form 8-K disclosure obligation would not provide for a reporting delay when there is an ongoing internal or external investigation related to the cybersecurity incident. While the SEC recognized that a delay in reporting could help facilitate law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident and preventing future cybersecurity incidents, the SEC's current view is that the importance of timely disclosure of cybersecurity incidents for investors would justify not providing for a reporting delay.

Cybersecurity Governance

Regulation S-K Item 106

Provide disclosure of (i) existing policies and procedures for the identification and management of cybersecurity incidents and (ii) the ***board's*** oversight of cybersecurity risk and ***management's*** role in assessing and managing cybersecurity-related risks.

When applicable, the description of the board's cyber-related oversight would include:

- whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks;
- the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and
- whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

When applicable, the description of the board's oversight would include:

- whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection and remediation of cybersecurity incidents, and the relevant expertise of such persons or members;
- whether the company has a designated a chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the company's organizational chart, and the relevant expertise of any such persons;
- the processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents; and
- whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.

Regulation S-K Item 407

Provide disclosure of directors' expertise in cybersecurity and a description of the nature of the expertise. The additional disclosure would require companies to consider prior work experience, education, knowledge, skills and other background experience.

Updates on Previously Reported Cybersecurity Incidents

If a company has previously provided disclosure regarding one or more cybersecurity incidents pursuant to new Item 1.05 of Form 8-K, disclose any material changes, additions, or updates regarding such incident in the company's Form 10-Q or Form 10-K for the period in which the change, addition, or update occurred.

Inline XBRL

Tag the information specified by proposed Item 1.05 of Form 8-K and Items 106 and 407(j) of Regulation S-K in Inline eXtensible Business Reporting Language (XBRL).

Preparing for the Final Rules

Here are a few takeaways that companies should be thinking about now to prepare for these potential new requirements:

- Given the four business day reporting deadline for disclosing material cybersecurity incidents, companies should evaluate their disclosure controls and procedures associated with the timing and reporting of cyber risks and incidents.
- Identify current directors with cybersecurity experience. Evaluate directors' prior work experience, education, knowledge, skills or other background experience relative to cybersecurity. Companies should consider whether their board, as currently composed, has adequate depth of cybersecurity experience in relation to the threat of cybersecurity incidents to their operations and financial condition. Where members of management or committees are responsible for managing cybersecurity risk, companies should evaluate the relevant expertise of such person or members. Update your annual director and officer questionnaire to identify cybersecurity-related experience.
- Consider the board and management's current role in overseeing the management of the company's cybersecurity risk and whether any updates should be made to the related policies and procedures.
- Identify and monitor the practices of third-party service providers who maintain investor or client information and are at risk from cyberattack. The proposed amendments would require companies to discuss whether the company has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third party service provider. Consider whether any practices or procedures need to be formalized or strengthened.
- Companies should continue to actively evaluate their cybersecurity programs and consider implementation of additional efforts to further cyber hygiene and prevent cybersecurity incidents, such as updating software regularly, adopting incident response plans, requiring employee training and mandating complicated passwords and multi-factor authentication to gain access to systems.

Impacted Forms

The below excerpt from the release's PRA Table 1 summarizes the forms and schedules affected by the proposed requirements.

Proposed Requirements and Effects	Affected Forms and Schedules
Form 8-K, Item 1.05 Require disclosure regarding cybersecurity incidents.	Form 8-K
Form 6-K, Item 1.05 Require disclosure regarding cybersecurity incidents.	Form 6-K
Adding Item 106 Disclosures Require disclosure regarding policies and procedures. (Item 106(b)) Require disclosure regarding board and management oversight of cybersecurity risk. (Item 106(c)) Require updated disclosure regarding cybersecurity incidents (Item 106(d))	Form 10-K Form 20-F Form 10-Q (Item 106(d))
Adding Item 407(j) disclosures Require disclosure on the cybersecurity expertise of members of the board of directors of the [company], if any.	Form 10-K Schedule 14A Schedule 14C

[1] Commissioner Hester M. Peirce expressed concerns that the proposal stepped outside of the SEC's Congressionally defined role and looked "more like a list of expectations about what issuers' cybersecurity programs should look like and how they should operate" in her dissenting statement.

[2] Consider, for example, the SEC's June 2021 settlement with First American Financial Corporation.

[3] Consider, for example, the SEC's August 2021 settlement with Pearson plc.

akingump.com