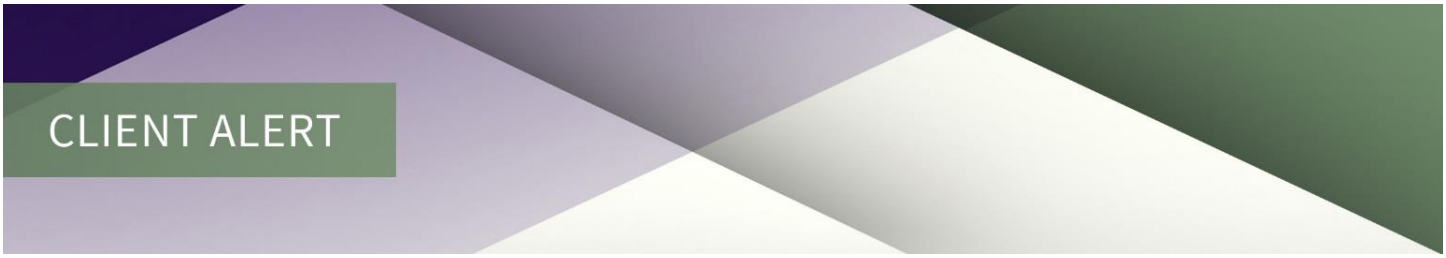
WILLKIE FARR & GALLAGHER LLP



SEC Proposes Cybersecurity Rules

March 15, 2022

AUTHORS

Daniel K. Alvarez | Elizabeth P. Gray | Robert B. Stebbins | Laura E. Jehl
Richard M. Borden | Michelle Bae | Marc J. Lederer

On March 9, 2022, the Securities and Exchange Commission (the "SEC" or the "Commission") voted 3-1 to propose rules requiring current reporting on Form 8-K of material cybersecurity incidents, and periodic reporting on Form 10-Q or Form 10-K of any material updates to the previously reported incidents.[1] Most notably, the SEC proposes to require a registrant to disclose a cybersecurity incident within four business days if the registrant determines the incident is material. In addition, a registrant would be required to provide in its Form 10-K disclosures about (A) its policies and procedures to identify and manage cybersecurity risk, (B) management's role and expertise in implementing the registrant's cybersecurity policies, procedures, and strategies, and (C) the board of directors' oversight role.[2] Finally, the proposed rules would require disclosure of the cybersecurity expertise of its directors, which disclosure would be made in the registrant's proxy or information statement when action is to be taken with respect to the election of directors, and in its Form 10-K.[3]

The SEC's proposals build upon its previously issued interpretive guidance, which was issued in 2018 to assist public companies in determining when they may be required to disclose information regarding cybersecurity risks and incidents under existing disclosure rules.[4]

1 *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Securities Exchange Act of 1934 (the "Exchange Act") Release No. 94382 (Mar. 9, 2022) (the "Proposing Release"), available here.

2 *Id.* at p. 19.

3 *Id.* at p. 19. A description of the filing requirements for foreign private issuers is set forth below.

4 *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 21, 2018) [83 FR 8166], available here.

Form 8-K Amendments—Material Cybersecurity Incidents.

The proposed amendments would add a new Item 1.05 to Form 8-K requiring a registrant to disclose information about a cybersecurity incident within four business days after the registrant determines that the incident is material. A registrant is required to make a materiality determination regarding the cybersecurity incident as soon as reasonably practicable after discovery thereof.

As to when an incident is "material," the Proposing Release points to the tests set forth in cases such as *Basic, Inc. v. Levinson* and *TSC Industries, Inc. v. Northway, Inc*.[5] "Cybersecurity incident" is defined broadly in the proposal: "an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."[6] "Information systems" is defined broadly to include any information resources owned or used by the registrant.

A registrant would be required to disclose in the Form 8-K the following about a material cybersecurity incident, to the extent the information is known at such time: (i) when the incident was discovered and whether it is ongoing; (ii) a description of the nature and scope of the incident; (iii) whether any data was stolen, accessed, altered or used for any unauthorized purpose; (iv) the effect of the incident on the registrant's operation; and (v) whether the registrant has remediated or is currently remediating the incident.[7]

The Proposing Release acknowledges that many states have laws that allow companies to delay providing public notice about a data breach incident or notifying certain constituencies of such an incident if law enforcement determines that notification will impede a civil or criminal investigation.[8] However, the SEC dismissed those concerns, stating that those state law obligations are distinct from companies' obligations to disclose material information to their shareholders under the federal securities laws. In addition, the SEC highlighted that, under the Proposing Release, a registrant is not required to publicly disclose specific, technical information about its planned response to the incident or its cybersecurity systems, or potential system vulnerabilities in detail. As such, the SEC believes that the required reporting under the Proposing Release would not impede the registrant's response or remediation of the incident, and therefore the Commission rejected

---

5 *Id.* at pp. 22-23. Information 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." *TSC Industries v. Northway*, 426 U.S. at 449. In articulating this materiality standard, the Supreme Court recognized that "[d]oubts as to the critical nature" of the relevant information "will be commonplace." But "particularly in view of the prophylactic purpose" of the securities laws, and "the fact that the content" of the disclosure "is within management's control, it is appropriate that these doubts be resolved in favor of those the statute is designed to protect," namely investors. *Id*. at 448.

6 *Id.* at p. 20.

7 *Id.* at p. 21.

8 *Id.* at pp. 25-26.

the possibility of a reporting delay when there is an ongoing internal or external investigation related to the cybersecurity incident. Instead, the Proposing Release focuses on the importance of prompt public disclosure of information regarding material cybersecurity incidents to investor protection and well-functioning, orderly, and efficient markets.[9]

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, so long as Form 8-K reporting is current at the time the Form S-3 or SF-3 is filed.[10]

The Proposing Release provides that new Item 1.05 would be included in the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) of the Exchange Act or Rule 10b-5 thereunder. Thus, no failure to file a report on Form 8-K that is required solely pursuant to Item 1.05 would be deemed a violation of Section 10(b) or Rule 10b-5.[11]

Form 10-K/10-Q Amendments—Cybersecurity Incidents, Risk Management and Strategy, and Governance.

The proposed amendments would require registrants to disclose any material change to the information previously disclosed under Item 1.05 of Form 8-K; any changes would be included in the Form 10-Q or Form 10-K (for the fourth fiscal quarter) for the respective fiscal quarter in which the material change occurred. However, the Proposing Release also notes that there may be situations where a registrant would need to file an amended Form 8-K to correct disclosure from the initial Form 8-K, such as when the disclosure in the initial Form 8-K becomes inaccurate or materially misleading as a result of subsequent developments.[12]

The proposed amendments would also require disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate. The required disclosure would be similar to the disclosure required under Item 1.05 of Form 8-K for a material cybersecurity incident. Disclosure would be required in the periodic report for the period in which the registrant has determined that they are material in the aggregate.[13]

On risk management, the proposed amendments would add new Item 106(b) of Regulation S-K, which would require the following Form 10-K disclosures by a registrant:

- whether it has a cybersecurity risk program and if yes, a description thereof;

---

9 *Id.*

10 *Id.* at p. 27.

11 *Id.* at p. 27.

12 *Id.* at pp. 32-33.

13 *Id.* at pp. 33-34.

- whether it engages third parties (such as assessors, consultants or auditors) in connection with any cybersecurity risk assessment program;
- whether it has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third party service provider, including policies and procedures addressing whether and how cybersecurity considerations affect the selection and oversight of these providers and mechanisms the company uses to mitigate cybersecurity risks related to these providers;
- whether it undertakes activities to prevent, detect and minimize effects of cybersecurity incidents;
- whether it has business continuity, contingency, and recovery plans in the event of a cybersecurity incident;
- whether previous cybersecurity incidents have led to changes in the registrant's governance, policies and procedures, or technologies;
- whether cybersecurity-related risk and incidents have affected or are reasonably likely to affect its results of operations or financial condition and if so, how; and
- whether cybersecurity risks are considered as part of its business strategy, financial planning, and capital allocation and if so, how.[14]

On governance, proposed Item 106(c) of Regulation S-K would require Form 10-K disclosure of a registrant's cybersecurity governance. As it pertains to the board's oversight of cybersecurity risk, Item 106(c)(1) would require disclosure of: (1) whether the entire board, certain board members or a board committee is responsible for the oversight of cybersecurity risks; (2) the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and (3) whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.[15]

Proposed Item 106(c)(2) would require a description of management's role in managing cybersecurity risks and in implementing the registrant's cybersecurity policies, procedures, and strategies. This description would include, but not be limited to, the following information:

- whether any management positions or committees are responsible for measuring and managing cybersecurity risk, and the relevant expertise of such persons;

---

[14] *Id.* at pp. 37-38.

[15] *Id.* at p. 39.

- whether the registrant has designated a chief information security officer, or someone in a comparable position, and if so, to whom that individual reports, and the relevant expertise of any such persons;
- the processes by which such persons are informed about and monitor cybersecurity incidents (including the prevention, mitigation, detection, and remediation thereof); and
- whether and how frequently such persons report to the board of directors or a committee of the board of directors on cybersecurity risk.[16]

Regulation S-K Amendments—Board Cybersecurity Experience.

The proposed amendments would add a new paragraph (j) to Item 407 of Regulation S-K, requiring disclosure about the cybersecurity expertise of members of the board of directors, if any. To the extent a board member has such expertise, disclosure would be required of the name of the director and of a description of the nature of the expertise. The Item 407(j) disclosure would be required in a registrant's proxy or information statement when action is to be taken with respect to the election of directors, and in its Form 10-K.

The Proposing Release does not define "cybersecurity expertise" but does include a non-exclusive list of factors that a registrant should consider in make a determination whether each director has such expertise, including (i) whether the director has prior work experience in cybersecurity, (ii) whether the director has obtained a degree in cybersecurity, and (iii) whether the director has knowledge, skills, or other background in cybersecurity (including in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning).[17]

Other Proposals.

Foreign Private Issuers. Foreign Private Issuers ("FPIs") are not required to file current reports on Form 8-K, but instead they are required to furnish on Form 6-K copies of all information that the FPI: (i) makes or is required to make public under the laws of its jurisdiction of incorporation, (ii) files, or is required to file under the rules of any stock exchange, or (iii) otherwise distributes to its security holders. The proposed amendments would amend Form 6-K to reference material cybersecurity incidents among the items that may trigger a current report on Form 6-K.[18]

The proposed amendments would add a new Item 16J to Form 20-F that would require an FPI to include in its annual report on Form 20-F the same type of disclosure that would be required in Items 106 and 407(j) of Regulation S-K and

[16] *Id.* at p. 40.

[17] *Id.* at p. 45. Any person who is identified as having expertise in cybersecurity under Item 407 will not be deemed an expert for purposes of Section 11 of the Securities Act of 1933, as amended.

[18] *Id.* at p. 26.

that would be required in periodic reports filed by domestic registrants. With respect to incident disclosure, where an FPI has previously reported an incident on Form 6-K, the proposed amendments would require an update regarding such incidents, consistent with proposed Item 106(d)(1) of Regulation S-K. In addition, amended Form 20-F would require FPIs to disclose on an annual basis information regarding any previously undisclosed material cybersecurity incidents that have occurred during the reporting period, including a series of previously undisclosed individually immaterial cybersecurity incidents that have become material in the aggregate.[19]

Inline XBRL. The proposed amendments would require registrants to tag the information specified by Item 1.05 of Form 8-K and Items 106 and 407(j) of Regulation S-K in Inline XBRL in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual.[20]

Dissenting Statement. Commissioner Hester Peirce issued a statement in dissent, arguing that the proposal, while couched in disclosure language, guides companies in substantive ways, by issuing requirements which function as a list of expectations about what issuers' cybersecurity programs should look like and how they should operate. In her view, the integration of cybersecurity expertise into corporate decision-making should be left to the judgment of the company, and not the SEC, which lacks necessary expertise in the area.[21] In addition, she noted that the governance disclosure requirements function as an "unprecedented micromanagement by the Commission of the composition of and functioning of both the boards of directors and management of public companies."[22] Finally, she noted a concern that the Commission was "unduly dismissive" of the need to cooperate with and at times defer to other governmental regulators, especially law enforcement agencies.[23]

More Cybersecurity Work Ahead.

With this action, the SEC appears to be looking at ways to improve not just disclosure by public companies of cybersecurity incidents, but also the cybersecurity programs and related disclosure controls of these companies. For example, while the Proposing Release focuses on public company disclosures and reporting, Commissioner Peirce's point that one anticipated side effect of the proposed amendments is that they likely would require public companies to develop comprehensive cybersecurity programs and related disclosure controls in accordance with the "disclosure requirements" set forth in the Proposing Release, is well-taken. Similarly, registrants likely would need to revisit their incident response plans to analyze each incident for materiality in a timely manner – a task that seems likely to be a

---

19 *Id.* at p. 48.

20 *Id.* at p. 49.

21 *See* Dissenting Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposal, Commissioner Hester M. Peirce (Mar. 9, 2022).

22 *Id.* at p. 1.

23 *Id.* at p. 2.

source of significant trepidation given that the extent or scope of a cybersecurity incident is often difficult to determine at the time the incident becomes known.

Comments on the proposed amendments must be received by the later of May 9, 2022 or 30 days after the Proposing Release is published in the Federal Register, and we anticipate many of the issues raised above will generate significant comment. In particular, while the SEC seemed to dismiss concerns about publicly disclosing incidents that may be under ongoing internal or external investigation, we would expect many registrants and other interested parties to object to the disclosure requirements while such investigations are ongoing. Likewise, there are a number of open questions. For example, the SEC left open significant questions as to how registrants assess cybersecurity events of service providers or other third parties.

Nevertheless, the types of requirements in the Proposing Release are consistent with recent SEC proposals for policies, procedures, disclosure and reporting for investment advisers and registered funds, and likely a harbinger of further activity with respect to cybersecurity. Chairman Gensler recently suggested that he anticipates more SEC rulemaking as to privacy, data security, and cybersecurity requirements with respect to broker-dealers, Regulation SCI, and intermediaries' requirements regarding customer notices (Regulation S-P).[24] We will continue to monitor these potential rulemakings and other legal developments as to cybersecurity.

[24] *See* Statement on Proposal for Mandatory Cybersecurity Disclosures (Mar. 9, 2022).

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Robert B. Stebbins
212 728 8736
rstebbins@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

Michelle Bae
212 728 3166
ebae@willkie.com

Marc J. Lederer
212 728 8624
mlederer@willkie.com