MAYER | BROWN

March 14, 2022

Legal Update

SEC Proposes New Rules on Public Company Cybersecurity Disclosures

Background

On March 9, 2022, the U.S. Securities and Exchange Commission (the "SEC") released proposed amendments (the "Proposed Amendments") aimed at enhancing and standardizing disclosure relating to cybersecurity risks and incidents. Under the existing regulatory framework, neither Regulation S-K nor Regulation S-X expressly requires that cybersecurity risk management procedures, cybersecurity risks or incidents be disclosed.[1] However, the SEC's Division of Corporation Finance published disclosure guidance in 2011,[2] which was followed by SEC interpretive guidance issued in 2018, explaining when registrants may be required to disclose information in SEC filings relating to cybersecurity risks and incidents under the principles-based disclosure framework, while considering the materiality of such risks and incidents.[3]

Despite improvements in the disclosure of material cybersecurity incidents and cybersecurity risk management procedures following the interpretive guidance, the SEC expressed concern that "current reporting may contain insufficient detail . . . is inconsistent, may not be timely, and can be difficult to locate."[4] To address these concerns, the Proposed Amendments would require more standardized and comparable disclosure from companies. If enacted, the Proposed Amendments will require public companies to report information relating to cybersecurity risk management, strategy, governance and material cybersecurity incidents. The proposed information required to be disclosed, the timing and the means of disclosure are summarized in the following table, with further discussion below:

Proposed Amendment	What to disclose	When to disclose
Item 1.05 on Form 8-K.	Material cybersecurity incidents: • 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 registrant's operations; and • Whether the registrant has remediated or is currently remediating the incident.	Disclose within four business days after the registrant determines it has experienced a material cybersecurity incident.

Proposed Amendment	What to disclose	When to disclose
Item 106(d)(1) of Regulation S-K.	Updates to previously filed Form 8-K disclosure on cybersecurity incidents. Non-exclusive examples of disclosure: • Any material impact of the incident on registrant's operations and financial condition; • Any potential material future impacts on registrant's operations and financial condition; • Whether the registrant has remediated or is currently remediating the incident; and • Any changes in the registrant's policies and procedures as a result of the incident, and how the incident may have informed such changes.	Disclose in the subsequent quarterly or annual report for the period in which the incident occurred (*i.e.*, Form 10-Q or 10-K, as applicable).
Item 106(d)(2) of Regulation S-K.	Disclosure required when a series of individually immaterial cybersecurity incidents become material when considered in the aggregate.	Disclose in the subsequent quarterly or annual report for the period in which the incidents occurred (*i.e.*, Form 10-Q or 10-K, as applicable).
Item 106(b) of Regulation S-K.	Registrant's policies and procedures to identify and manage cybersecurity risks.	Disclose in registrant's annual report (*i.e.*, Form 10-K).
Item 106(c)(1) of Regulation S-K.	Board of Directors' cybersecurity expertise and oversight of cybersecurity risk.	Disclose in registrant's annual report (*i.e.*, Form 10-K).
Item 106(c)(2) of Regulation S-K.	Management's role in implementing cybersecurity policies and procedures.	Disclose in registrant's annual report (*i.e.*, Form 10-K).
Item 407(j) of Regulation S-K.	The name of the registrant's Director with cybersecurity expertise (if any) and details as necessary to fully describe the nature of that Director's expertise.	Disclose in registrant's annual report (*i.e.*, Part III of Form 10-K). Disclose in a registrant's proxy or information statement when action is to be taken regarding the election of directors (*i.e.*, Schedule 14A or Schedule 14C).
Amendments affecting Foreign Private Issuers		
Amendment to General Instruction B of Form 6-K.	Cybersecurity incidents now included as a reporting topic.	Disclose timely, in a manner consistent with the general purpose and use of Form 6-K.
Item 16J on Form 20-F.	Substantively the same as Items 106 and 407(j) as above.	Disclose in foreign private issuer's annual report only (*i.e.*, Form 20-F).

Proposed Amendments

The summary table indicates the information that issuers would be required to disclose under the Proposed Amendments, if adopted.

Below, we discuss certain of these proposed additional requirements in more detail.

New Item 1.05 on Form 8-K for material cybersecurity incidents. The SEC proposes to include a new Item 1.05 on Form 8-K, requiring registrants to disclose information about a cybersecurity incident within four business days after the registrant determines that it has experienced a material cybersecurity incident. A proposed Instruction to Item 1.05 requires that determinations of materiality be made "as soon as reasonably

practicable after discovery of the incident." The Proposed Amendments would require a registrant to disclose the following information about a material cybersecurity incident, if known at the time of filing:

- 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 registrant's operations; and
- Whether the registrant has remediated or is currently remediating the incident.

In the Proposing Release, the SEC stated that the registrant would not be expected to publicly disclose specific, technical or other information about its planned response that could impede the response or remediation of the incident.

In determining whether a cybersecurity incident is "material," the SEC proposed to apply the existing standard of materiality under the federal securities laws; that is, 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."[5] The SEC also provided a non-exclusive list of example cybersecurity incidents that may be determined to be material, triggering the proposed disclosure requirement under Item 1.05.

The SEC's proposal, if adopted in its current form, would dramatically alter a factor often at play in cybersecurity incident response – so-called "law enforcement delays" that are provided for in many state data breach notification laws. These provisions allow companies, at the request of law enforcement, to delay providing required notifications to regulators or individuals to facilitate ongoing investigations. The Proposing Release acknowledges such provisions, but expressly clarifies that Form 8-K reporting obligations would be triggered even where a delay was requested by law enforcement.[6]

The Proposing Release notes the SEC's belief that any delay provision would undermine the purpose of the disclosure requirement and that, on balance, the importance of timely disclosure overrides any need for delay.[7]

Because foreign private issuers are not required to file current reports on Form 8-K, the SEC proposes a similar amendment to Form 6-K to amend General Instruction B thereto and to include material cybersecurity incidents as an event that may trigger a current report on Form 6-K. Additionally, the SEC proposed to amend General Instruction I.A.3.(b) of Form S-3 and General Instruction I.A.2 of Form SF-3 such that a late filing on Form 8-K regarding the new item 1.05 would not cause the registrant to lose eligibility for Form S-3 or SF-3.

New Item 106(d) of Regulation S-K for Disclosure of Cybersecurity Incidents in Periodic Reports.
Proposed Item 106(d) of Regulation S-K would require disclosure of cybersecurity incidents in a registrant's periodic reports on Forms 10-Q and 10-K. Proposed Item 106(d)(1) would require registrants to disclose "any material changes, additions or updates to information required to be disclosed pursuant to Item 1.05 of Form 8-K" in the registrant's quarterly report filed on Form 10-Q or annual report filed on Form 10-K. Information that was not available at the time of the initial Form 8-K filing would be disclosed in the registrant's subsequent periodic filing. Item 106(d)(1) also provides a non-exclusive list of information to be provided, as applicable, including the effect of the previously reported cybersecurity incident and a description of remedial steps the registrant has taken or plans to take.

Proposed Item 106(d)(2) would require disclosure when a series of cybersecurity incidents that are immaterial when considered individually become material in the aggregate. As proposed, Item 106(d)(2) would require a registrant to analyze the materiality of related cybersecurity incidents on both an individual and an aggregate basis. The effect of Item 106(d)(2) would be that if the registrant determines the incidents to be material in the aggregate, then the registrant would have to disclose the incident in its periodic reports, even if the incidents would not warrant disclosure individually.

Required Disclosures Specified in Proposed Item 106. Proposed Item 106 of Regulation S-K would require detailed disclosures regarding (i) policies and procedures, if any, for identifying and managing cybersecurity risks and the company's cybersecurity governance, (ii) the board of directors' role in oversight of cybersecurity risks and (iii) management's role in managing cybersecurity-related risks and implementing the company's cybersecurity policies and procedures.

Proposed Item 106(b) provides that disclosure regarding a registrant's cybersecurity policies and procedures should include the following:

- Whether the registrant has a cybersecurity risk assessment program, and if so, a description of such program;
- Whether the registrant engages assessors, consultants, auditors or other third parties in connection with any cybersecurity risk assessment program;
- Whether the registrant undertakes activities to prevent, detect and minimize effects of cybersecurity incidents;
- Whether the registrant has business continuity, contingency and recovery plans in the event of a cybersecurity incident; and
- Whether cybersecurity-related risk and incidents have affected or are likely to affect the registrant's operations or financial condition, and if so, how.

Proposed Item 106(c)(1) provides that disclosures with respect to board oversight should include the following:

- Whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risk;
- 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 considers cybersecurity risks as part of its business strategy, risk management and financial oversight.

Proposed Item 106(c)(2) provides that disclosures regarding management's role should include the following:

- Whether certain management positions or committees are responsible for managing cybersecurity risk, and the relevant expertise of such persons;
- Whether the registrant has a designated 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 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.

New Item 407 of Regulation S-K for Disclosure of Cybersecurity Expertise of Directors. Under the proposed amendment to Item 407 of Regulation S-K, a registrant would be required to disclose whether any board member has cybersecurity expertise, and, if so, the nature of such expertise. Item 407(j) would not define what constitutes "cybersecurity expertise," but would include a non-exclusive list of criteria that should be considered, including prior work experience,[8] possession of a cybersecurity certification or degree or other knowledge, skills or background in cybersecurity. Additionally, Item 407(j)(2) would state that a person who is determined to have expertise in cybersecurity will not be deemed an expert for any purpose, including for purposes of Section 11 of the Securities Act.

Periodic Disclosures by Foreign Private Issuers. The Proposed Amendments would generally affect most foreign private issuers. Form 20-F would be amended by adding Item 16J to require the same type of disclosure that is proposed for domestic registrants in Items 106 and 407(j) of Regulation S-K. For example, with respect to incident disclosure, if a foreign private issuer previously reported a cybersecurity incident on Form 6-K, it would be required to provide an update of such incident on Form 20-F, consistent with proposed Item 106(d)(1) of Regulation S-K.

The multijurisdictional disclosure system ("MJDS") generally permits eligible Canadian foreign private issuers to use Canadian disclosure standards and documents to satisfy the SEC's registration and disclosure requirements. The SEC therefore did not propose prescriptive cybersecurity disclosure requirements for Form 40-F filers. However, the SEC requested comment as to whether it should require an MJDS issuer filing an annual report on Form 40-F to comply with the SEC's specific proposed cybersecurity-related disclosure requirements in the same manner as Form 10-K or Form 20- F filers.

Data Requirements. The SEC proposed that all forms and disclosures described above be tagged in Inline XBRL in order to facilitate comparison and analysis of the data being disclosed.

Practical Considerations

The Proposed Amendments, if adopted in the form in which they have been proposed, will result in companies that have suffered a cybersecurity incident having less flexibility in deciding when, how and what information to disclose. By limiting a company's flexibility and by providing fairly prescriptive guidance regarding the types of disclosures that are expected through the non-exclusive lists included in the Proposing Release, the result achieved may be the opposite of what was intended. Premature disclosures made within four days' time, before a company may have had an adequate opportunity to make important and complex assessments, may result in disclosures that are overly broad and generic, and may be more misleading than informative. The possibility to supplement or correct these in subsequent filings should provide scant comfort to certifying officers and a board of directors. Additionally, the Proposed Amendments regarding cybersecurity risk oversight disclosure are prescriptive, requiring detailed disclosure about members of the board of directors, management and their interactions. While the SEC regulates disclosure, and not behavior, these Proposed Amendments, if adopted, have the potential to steer behavior in a particular direction in order to result in disclosure that reads favorably

by comparison to peer companies. For example, while the Proposed Amendments would not require each company to have a cybersecurity expert on its board of directors, companies may begin to prioritize identifying candidates with cybersecurity expertise before other characteristics in order to avoid providing disclosure that suggests the company does not have adequate cybersecurity oversight.

In our recent alert, we reported on the Investment Management Cybersecurity Proposing Release, which affects business development companies ("BDCs"). These Proposed Amendments also affect BDCs. BDCs may need to provide similar disclosures if subject to both sets of proposed amendments, which is duplicative and expensive.

The Proposed Amendments are subject to a 60-day comment period following issuance or a 30-day period following publication of the Proposing Release in the Federal Register, whichever period is longer. This means that the comment period is open until at least May 9, 2022. The Proposing Release raises many questions for comment. Interested parties should assess as soon as possible whether they want to submit a comment letter to highlight issues that are of particular interest to them, and if so, begin work on any such comment letter promptly.

See the Proposed Amendments and the related Fact Sheet and SEC announcement.

For more information about the topics discussed in this Legal Update, please contact any of the following authors.

Kimberly Ayudant
+1 212 506 2156
kayudant@mayerbrown.com

Rajesh De
+1 202 263 3366
rde@mayerbrown.com

Marc Leong
+1 212 506 2468
mleong@mayerbrown.com

Vivek K. Mohan
+1 650 331 2054
vmohan@mayerbrown.com

Anna T. Pinedo
+1 212 506 2275
apinedo@mayerbrown.com

Laura D. Richman
+1 312 701 7304
lrichman@mayerbrown.com

Christina M. Thomas
+1 202 263 3344
cmthomas@mayerbrown.com

The Free Writings & Perspectives, or FW&Ps, blog provides news and views on securities regulation and capital formation. The blog provides up-to-the-minute information regarding securities law developments, particularly those related to capital formation. FW&Ps also offers commentary regarding developments affecting private placements, mezzanine or "late stage" private placements, PIPE transactions, IPOs and the IPO market, new financial products and any other securities-related topics that pique our and our readers' interest. Our blog is available at: www.freewritings.law.

ENDNOTES

[1] *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038; 34-94382; IC-34529; File No. S7-09-22 (Mar. 9, 2022), available at www.sec.gov/rules/proposed/2022/33-11038.pdf ("Proposing Release").

[2] *See* CF Disclosure Guidance: Topic No. 2- Cybersecurity (Oct. 13, 2011), available at www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[3] *See* SEC Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 26, 2018) No. 33-10459 (Feb. 21, 2018) [83 FR 8166], available at www.sec.gov/rules/interp/2018/33-10459.pdf.

[4] Proposing Release, at 17.

[5] *TSC Industries, Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1976).

[6] *See* Proposing Release, at 25-26.

[7] *Id.*

[8] The Proposing Release references prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager or business continuity planner.