CARTER LEDYARD

our resources

SEC Adopts New Cybersecurity Disclosure Rules for Public Issuers

July 31, 2023

The Securities and Exchange Commission (the "**SEC**") announced on July 26, 2023 that it has adopted its much-anticipated new cybersecurity rules for public companies. The new rules require issuers to promptly disclose the impacts of material cybersecurity incidents and disclose on an annual basis material information regarding cybersecurity risk management, strategy, and governance.

We previously reported on the rule proposals. Following extensive comments over the last 12 months, some of the proposals were not adopted and issuers now have fewer disclosure obligations than previously envisioned, as outlined below. Nevertheless, these new rules are significant and reporting companies must be prepared to comply.

New 8-K Item

The rules add a new Item 1.05 to Form 8-K, which mandates that issuers report any **cybersecurity incident** determined to be material within four business days after the determination. Issuers must describe the material aspects of the incident's nature, scope, and timing, as well as its material impact or reasonably likely material impact on the issuer, including its **financial condition and results of operations**.

An issuer's **materiality determination** regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident. To the extent that the information called for in Item 1.05 is not determined or is unavailable at the time of the required filing, the issuer must include a statement to this effect in the filing and then must file an amendment to its Form 8-K filing containing such information **within four business days** after the company, without unreasonable delay, determines such information or within four business days after such information becomes available.

In determining materiality, Item 1.05 requires consideration of the likely material impact on a company's "financial condition and results of operations" as well as other qualitative factors and quantitative factors. As an example, "harm to a company's reputation, customer or vendor relationships, or competitiveness" may be examples of a material impact on the issuer." Similarly, the "possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities" may constitute a reasonably likely material impact.

"*Cybersecurity incident*" is defined as an unauthorized occurrence, or a series of related unauthorized occurrences, 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.

There is no exemption for providing disclosures regarding cybersecurity incidents on third-party systems, nor any safe harbor for information disclosed about third-party systems.

The disclosure may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. The SEC indicated that the SEC and Department

of Justice ("**DOJ**") have developed an interagency communication process to facilitate this delay, and DOJ will notify affected issuers directly if they are subject to the delay. Time will tell how this exemption will work in practice given the tight timeline.

The disclosure is required to be tagged in Inline XBRL. Untimely filing of an Item 1.05 Form 8-K will *not* result in the loss of Form S-3 eligibility.

Form 10-K: New Regulation S-K Item 106

The new rules add a new Regulation S-K Item 106, which requires issuers to describe their processes, if any, for assessing, identifying, and managing **material** risks from **cybersecurity threats**, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents. Item 106 requires issuers to describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

"*Cybersecurity threat*" is defined as any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

Form 6-K

For foreign private issuers ("**FPIs**"), Form 6-K is being amended to require FPIs "to furnish information on material cybersecurity incidents that they make or are required to make public or otherwise disclose in a foreign jurisdiction to any stock exchange or to security holders."

Form 20-F

For FPIs, Form 20-F is being amended to require FPIs to make comparable periodic disclosure (similar to S-K Item 106).

Form 40-F

For Canadian issuers filing under the Multijurisdictional Disclosure System (MJDS), the SEC agreed *not* to amend Form 40-F, maintaining that Canadian issuers eligible to use MJDS should be permitted to follow their domestic disclosure standards, consistent with other disclosure requirements for those issuers.

Changes from the Initial Proposals

With respect to incident disclosure, the final rules "narrow the scope of disclosure," focusing on **the impact or reasonably likely impact of the incident,** rather than on the details of the incident itself, such as remediation status. The final rules also include the limited delay for disclosures that would pose a substantial risk to national security or public safety, require certain updated incident disclosure on an amended Form 8-K (instead of Forms 10-Q and 10-K) for domestic issuers and on Form 6-K (instead of Form 20-F) for FPIs, and omit the proposed aggregation of immaterial incidents for materiality analyses, instead defining cyber incident to include a "series of related unauthorized occurrences." With respect to the annual disclosure, the final rules "streamline the proposed disclosure elements related to risk management, strategy, and governance." In addition, **the SEC did not adopt the much-debated proposed requirement to disclose board cybersecurity expertise.**

Effectiveness

The final rules will become effective 30 days following publication of the adopting release in the Federal Register. The Form 10-K and Form 20-F disclosures will be due beginning with annual reports for fiscal years ending on or after December 15, 2023. The Form 8-K and Form 6-K disclosures will be due beginning the later of 90 days after the date of publication in the Federal Register or December 18, 2023. Smaller reporting companies will have an additional 180 days before they must begin providing the Form 8-K disclosure. With respect to compliance

with the structured data requirements, all registrants must tag disclosures required under the final rules in Inline XBRL beginning one year after initial compliance with the related disclosure requirement.

How to Prepare

Public issuers should verify that they have **procedures** in place to allow their teams conducting investigations of **cybersecurity threats** or **breaches** to timely convey the details to their officers responsible for making public disclosures related to cybersecurity.

Companies should confer with legal, compliance, and technology professionals to assess the materiality of a discovered **cybersecurity incident** and determine any disclosure obligations.

* * *

related professionals

Guy Ben-Ami / Partner
D 212-238-8658
benami@clm.com

Steven J. Glusband / Partner
D 212-238-8605
glusband@clm.com

Matthew D. Dunn / Partner
D 212-238-8706
mdunn@clm.com

Jodutt Marwan Basrawi / Associate
D (212) 238-8767
basrawi@clm.com