July 31, 2023

SEC Adopts Final Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

By Bruce Newsome, Kit Addleman, and Kierra Jones

On July 26, 2023, the Securities and Exchange Commission ("SEC") adopted new final rules and form amendments (the "Rules") addressing cybersecurity incidents as well as cybersecurity risk management, strategy, and governance. The Rules are designed to enhance and standardize the cybersecurity-related disclosure required by public companies subject to the reporting requirements of the Securities Exchange Act of 1934. The Rules will apply to companies that file on Forms 8-K and 10-K ("Domestic Filers"), including smaller reporting companies, as well as foreign private issuers that file on Forms 6-K and 20-F ("FPIs").

The Rules include amendments to (i) Form 8-K through the addition of Item 1.05, (ii) Form 10-K through the addition of Item 106 to Regulation S-K and (iii) Forms 6-K and 20-F, providing for generally parallel disclosure requirements for FPIs. Notably, in response to comments, the SEC scaled back a number of the disclosure requirements that were described in the proposed rules. Nevertheless, we expect that the new rules will be challenging for public companies to comply with—especially the requirement to report material cybersecurity incidents within four business days.

Domestic Filers, including smaller reporting companies, and FPIs will be required to include the periodic report disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. Current report disclosures (Form 8-K and Form 6-K) will be required beginning the later of 90 days after the date of publication of the adopting release in the Federal Register or December 18, 2023. However, smaller reporting companies will be allowed an additional 180 days for current report disclosures on Form 8-K; which, at the latest, would be by June 15, 2024.

New Current Report Disclosure Requirements

Form 8-K: Item 1.05. Material Cybersecurity Incidents.

Information Required to Be Disclosed. New Item 1.05 to Form 8-K will require companies to describe, to the extent known at the time of filing, the material aspects of the nature, scope, and timing of a cybersecurity incident, and the material impact or reasonably likely material impact on the company, including on its financial condition and results of operations. The Rules focus the disclosure on the material *impacts* of a material cybersecurity incident, and not on the specific details about the incident beyond the incident's basic identifying details. The materiality determination should consider the unique characteristics of the company and reflect an informed and deliberative process.

Companies must also disclose whether information required by Item 1.05 has not been determined or is unavailable at the time of filing. If such information is not initially available, companies must subsequently file an amendment to the Form 8-K within four business days after determining such information or it becomes available.

The SEC narrowed the scope of information required to be disclosed from that originally proposed and stated that this should lessen the burden of disclosure. For example, companies are not required to disclose remediation status, whether the incident is ongoing, or whether data was compromised unless the

circumstances of a particular cybersecurity incident require discussion of these aspects following a company determination that such aspects are material to understanding the cybersecurity incident or its impact. In addition, Instruction 4 to Item 1.05 provides that companies are not required to disclose specific or technical information about its planned response to the cybersecurity incident, its cybersecurity systems, potential system vulnerabilities or such other detail that "would impede the company's response or remediation of the incident."

Multiple Cybersecurity Incidents. The SEC did not adopt any requirement to aggregate immaterial cybersecurity incidents to determine if in the aggregate, disclosure would be required. However, the SEC noted that the definition of "cybersecurity incident" extends to "a series of related unauthorized occurrences," such as where (i) the same person engages in a number of smaller but continuous cyberattacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material, or (ii) a series of related attacks from multiple persons exploiting the same vulnerability collectively impedes the company's business materially.

Form 8-K Due Date. A filing under Item 1.05 will be due four business days after the company determines the cybersecurity incident is material, considering both quantitative impacts as well as qualitative impacts (such as harm to the company's reputation, customer relationships, vendor relationships, competitive position, and the possibility of litigation or regulatory investigations or actions). In addition, companies must make such materiality determination "without unreasonable delay." In this regard, the SEC noted that the inability to determine the full extent of an incident because of the nature of the incident or the company's systems, or otherwise the need for continued investigation regarding the incident, should not delay the company from determining materiality. However, a decision to share information with another company or government actors does not necessarily mean a materiality determination has been made.

Impact of Late Filing on Form S-3 Eligibility. The SEC has provided that a late Form 8-K filing under Item 1.05 will not result in a loss of eligibility to file a Form S-3.

Exception for Delayed Filing. Due to substantial risks to national security or public safety, the SEC has allowed for filing delays if the U.S. Attorney General determines, and notifies the SEC in writing, that disclosure would pose such risks. An initial 30-day delay may be extended by 30 more days if disclosure continues to pose a substantial risk to national security or public safety. In extraordinary circumstances, a final additional 60-day delay may be granted. Any additional requests beyond the 60-day delay would be subject to SEC consideration and such relief may be granted through exemptive order.

Form 8-K Amendments. If at the time of filing of the Form 8-K, certain required information is not determined or available, the company must file an amendment to its Form 8-K within four business days after the company determines such information or it becomes available. Other than with respect to such previously undetermined or unavailable information, the final rules do not separately create or otherwise affect a company's duty to update its prior statements. However, the SEC noted that companies may have (i) a duty to correct prior disclosure that the registrant determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made (for example, if the company subsequently discovers contradictory information that existed at the time of the initial disclosure) or (ii) a duty to update disclosure that becomes materially inaccurate after it is made (for example, when the original statement is still being relied on by reasonable investors).

Liability. Information provided pursuant to Item 1.05 will be considered "filed" instead of "furnished." As a result, companies may be subject to liability to investors in actions brought under Section 18 of the Exchange Act and

Section 11 of the Securities Act of 1933 to the extent the information is incorporated by reference into filings under the Securities Act.

XBRL Tagging. Companies must provide the required information in Inline XBRL-tagged format beginning one year after the initial compliance date.

Foreign Private Issuers. FPIs will be required to comply with generally parallel disclosure requirements, with such information to be reported on Form 6-K. However, for a cybersecurity incident to trigger a disclosure obligation on Form 6-K, the registrant must determine that the incident is material, in addition to meeting the other criteria for required submission of the Form 6-K.

New Disclosure Requirements for Forms 10-K and 20-F

Risk Management and Strategy

Domestic Filers.Domestic Filers will be required to provide in their annual reports on Form 10-K a description of their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes (Item 106 of Regulation S-K). Notably, the SEC narrowed the required scope of disclosure from that in the proposed rules based on comment letters.

A company should address the elements listed below, as well as any information it deems necessary for a reasonable investor to understand its cybersecurity processes:

- Whether and how the described cybersecurity processes have been integrated into the company's overall risk management system or processes;
- Whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes (but the names of the third parties and the services they provide are not required to be disclosed); and
- Whether the company has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.

Additionally, companies must provide a description of whether any risks from cybersecurity threats, including those resulting from previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, including its impact on business strategy, results of operations, or financial condition.

Foreign Private Issuers. FPIs have generally parallel disclosure requirements with respect to the Form 20-F.

Governance

The Rules will require descriptions of the roles of the board of directors and management in overseeing and implementing cybersecurity processes, and assessing and managing cybersecurity-related risks. The SEC generally narrowed the scope of the governance disclosures as compared to the proposed rules.

Board Oversight. A company must identify any board committee or subcommittee responsible for oversight and describe the processes by which the board or such committee is informed of such risks.

Management Oversight. Item 106(c)(2) provides a non-exhaustive list of elements to consider when disclosing management's role in assessing and managing the company's material risks from cybersecurity threats. The list includes the following:

- Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
- The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
- Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Materiality of Risks. Notably, the SEC did not qualify the disclosure of board oversight of cybersecurity risks by "material" because, if a board of directors determines to oversee a particular risk, the fact of such oversight being exercised by the board is material to investors. By contrast, management oversees many more matters and management's oversight of non-material matters is likely not material to investors, and as a result, a materiality qualifier is appropriate with respect to management oversight.

Director Cybersecurity Expertise. The SEC did not adopt a requirement to disclose director cybersecurity expertise in the final rules.

Foreign Private Issuers. FPIs must comply with the aligned requirements provided for in Form 20-F.

Key Definitions

"Cybersecurity incident" means 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.

"Cybersecurity threat" means 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.

"Information systems" means electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

Compliance

Domestic Filers will be required to include the periodic report disclosures in Form 10-K and FPIs on Form 20-F beginning with annual reports for fiscal years ending on or after December 15, 2023. Incident report disclosures on Form 8-K and Form 6-K will be required beginning the later of 90 days after the date of publication in the Federal Register or December 18, 2023. Smaller reporting companies have an additional 180 days and must begin complying with Form 8-K Item 1.05 on the later of 270 days from the effective date of the Rules or June

15, 2024. All companies must tag disclosures required under the final rules in Inline XBRL beginning one year after the initial compliance with the related disclosure requirement.

Potential Enforcement Consequences

Enforcement actions by the SEC in recent years addressing cyber disclosures suggest that the new Rules will be a focus for future enforcement investigations and litigation. Companies should be alert to the potential for misstatements and omissions in disclosures concerning cyber incidents and risk, as well as controls failures that have previously resulted in penalties and sanctions.

As one example, on June 15, 2021, the SEC announced that a California-based real estate settlement services company agreed to pay a civil money penalty of $487,616 in an enforcement action in which the SEC found that the company (i) failed to timely remediate a known vulnerability associated with a software application that stored and transmitted images of customers' title and escrow-related documents, which often contain non-public personal and financial information, and (ii) subsequently issued public disclosures about the vulnerability without fully evaluating the company's cybersecurity responsiveness and the magnitude of the risk posed by the vulnerability.[1] Indeed, at the time of its disclosures, the SEC found that that company did not actually have any disclosure controls and procedures related to cybersecurity, including incidents involving potential breaches of data, which led to the company's senior executives approving disclosures without material information regarding the vulnerability.

On August 16, 2021, a London-based public company that provides educational publishing and other services to schools and universities settled an SEC enforcement action and agreed to pay a civil money penalty of $1 million. The SEC found that the company claimed in its semi-annual report that there was the "hypothetical risk" of a data privacy incident but failed to disclose a 2018 data breach that actually occurred and resulted in the theft of data and login credentials from 13,000 customer accounts.[2] Worse still the SEC found the company had known about the vulnerability that allowed the breach but failed to address it for six months. The company also issued a media statement in July 2019 that mischaracterized the nature of the breach and the amount and type of data involved.

More recently on March 9, 2023, the SEC announced that a South Carolina-based public company that provides donor data management software to non-profit organizations agreed to pay $3 million for similarly making misleading disclosures about a 2020 ransomware attack that impacted more than 13,000 customers.[3] In particular, the SEC found that company did not have policies or procedures in place to ensure senior management was informed about the types of data accessed in the attack. As a result, the company's disclosures failed to disclose the material fact that the attacker exfiltrated unencrypted donor bank account information and social security numbers.

These enforcement actions are just a sampling of those which imposed penalties for disclosure and controls failures related to cybersecurity. With the new Rules providing additional specificity on the requirements for

[1] *See* Press Release, Sec. & Exch. Comm'n, SEC Charges Issuer With Cybersecurity Disclosure Controls Failures (June 15, 2021), https://www.sec.gov/news/press-release/2021-102.
[2] *See* Press Release, Sec. & Exch. Comm'n, SEC Charges Pearson plc for Misleading Investors About Cyber Breach (Aug. 16, 2021), https://www.sec.gov/news/press-release/2021-154.
[3] *See* Press Release, Sec. & Exch. Comm'n, SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors (Mar. 9, 2023), https://www.sec.gov/news/press-release/2023-48.

incident disclosures as well as cyber-related governance and procedures, future enforcement attention is expected to increase in those areas.

Conclusion

In advance of the compliance dates of the Rules, companies should begin evaluating and modifying to the extent necessary their existing internal processes and controls relating to cybersecurity threats and incidents to ensure timely compliance with the Form 8-K and Form 6-K accelerated disclosure requirements, as well as the related disclosure that will be required beginning with the 2023 Forms 10-K or 20-F for calendar year companies.

The adopting release for the Rules can be found here. For further information regarding disclosure, compliance and governance questions, please contact a member of the Haynes and Boone Capital Markets and Securities Practice Group. For additional information regarding enforcement consequences and data breach responses for public companies, please contact a member of Haynes and Boone's SEC Enforcement Group.