msk

sec approves new rules for cybersecurity disclosure and incident reporting

Blake Baron & Gabriel Miranda
MSK Client Alert

August 3, 2023

On July 26, 2023, the U.S. Securities and Exchange Commission ("SEC") adopted the new highly-anticipated cybersecurity disclosure rules for public companies.

Background:

Cybersecurity disclosure has been on the SEC's radar since their 2018 cybersecurity disclosure guidance. And, on March 9, 2022, the SEC first proposed its new cybersecurity rules for public companies aiming to "better inform investors" about public companies' "risk management, strategy, and governance and to provide timely notification to investors of material cybersecurity incidents."[1]

In last year's press release announcement of the proposed rules on cybersecurity, SEC Chair Gary Gensler noted that "[o]ver the years, [the SEC's] disclosure regime has evolved to reflect evolving risks and investor needs."[2] While supporting the proposed amendments, he added that "[a] lot of issuers already provide cybersecurity disclosure to investors. I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner."[3]

The final rules adopted will require current reporting on Form 8-K (or Form 6-K for foreign private issuers) for material cybersecurity events and an annual disclosure on Form 10-K (or Form 20-F for foreign private issuers) about corporate risk management, strategy, and governance of cybersecurity. Quarterly disclosure under Form 10-Q is no longer mandatory, as it was per the proposed rules, and there is no longer a requirement to identify a board cybersecurity expert.

attorneys

Blake Baron

Gabriel Miranda

practice areas

corporate & business transactions

cybersecurity and privacy

Form 8-K and Form 6-K Reporting:

Under the final rules, new Item 1.05 of Form 8-K will require disclosure, within four business days of the occurrence, of "any cybersecurity incident experience that is determined to be material,"[4] and to describe certain material aspects of such incident, such as the nature, scope and timing of the incident, as well as the impact or reasonably likely impact of the cybersecurity incident, including its financial implications. Registrants will be required to amend a prior Item 1.05 Form 8-K to disclose any information called for the new Item 1.05 that may not have been determined or available at the time of the initial filing.

Based on comments sent to the SEC on their first proposed rule in 2022, the final rule will require registrants to determine the materiality of these cybersecurity incidents "without unreasonable delay"[5] after discovery of the incident, and if the incident is determined to be material, registrants will have four business days to report it. According to the SEC, this final instruction language is intended to address concerns that the previously proposed instruction could result in undue pressure on registrants to make a materiality determination before having sufficient information to do so while "providing registrants notice that, though the determination need not be rushed prematurely, it cannot be unreasonably delayed in an effort to avoid timely disclosure."[6] So, registrants will be allowed limited leeway in making their materiality determination to avoid premature disclosure, except for rare cases where the disclosures would pose a substantial risk to national security or public safety. The untimely filing of an Item 1.05 Form 8-K will not affect a registrant's Form S-3 eligibility.

For foreign private issuers, Form 6-K was amended to now include "material cybersecurity incidents" to the list in General Instruction B of the information required to be furnished on Form 6-K.

Form 10-K and Form 20-F Reporting:

The final rules also introduced a new Item 106 to Regulation S-K, focusing on cybersecurity risk management, strategy and governance. Registrants will need to describe "their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition."[7]

Item 106 will also require registrants to describe the board of directors' oversight of cybersecurity risks and management's role in assessing and managing such risks, including:

- whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant 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.

Effective Dates:

The final rules will become effective on August 25, 2023. The Form 8-K and Form 6-K reporting requirements will apply to cybersecurity incidents occurring on or after December 18, 2023, with the exception of smaller reporting companies, which will not have to disclose incidents under Item 1.05 until June 15, 2024. The annual reporting requirement on Form 10-K or 20-F is applicable to all registrants, and will take effect for fiscal years ending on or after December 15, 2023.

In preparation to the foregoing new cybersecurity disclosure requirements, registrants should ensure that any incident plan response or other material policy dealing with cybersecurity incident responses is evaluated and adjusted, as needed, to reflect materiality cybersecurity incident determination processes, and other internal processes necessary to evaluate ongoing materiality of cybersecurity incidents. Further, registrants should also begin reviewing, and/or establishing, cybersecurity risk management, strategy and governance practices in light of these new disclosure obligations that will be included in upcoming Annual Reports on Form 10-K and 20-F.

Please contact the MSK Corporate & Business Transactions Department to discuss how we can help you comply with the new SEC cybersecurity disclosure obligations.

[1] U.S. Securities and Exchange Commission Press Release, dated March 9, 2022, "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies." (https://www.sec.gov/news/press-release/2022-39)

[2] See id.

[3] See id.

[4] U.S. Securities and Exchange Commission Release No. 33-11216 (https://www.sec.gov/files/rules/final/2023/33-11216.pdf).

[5] See id.

[6] See id.

[7] See id.