SEC ADOPTS FINAL RULES FOR CYBERSECURITY DISCLOSURES

Date: 7 August 2023

US Corporate Alert

By: Julie F. Rizzo, Tyler G. Anders, Kylie S. Herring, Desiree F. Moore

Companies will soon face new reporting requirements with respect to cybersecurity incidents and governance after the US Securities and Exchange Commission (SEC) adopted final rules on 26 July 2023. The final rules supplement prior disclosure guidance from 2011 and 2018, adding an affirmative obligation to disclose cybersecurity incidents and centralizing disclosures relating to cybersecurity risk management, strategy, and governance.

FORM 8-K/CYBERSECURITY INCIDENT REPORTING

The SEC added new Item 1.05 to Form 8-K that will require companies to report a cybersecurity incident within four business days of determining the incident is material. The focus of this reporting requirement is on the impact of the incident on the company and not on the details of the incident so as not to compound any security threats. Companies must determine whether a cybersecurity incident is material “without unreasonable delay” and should err on the side of making disclosure under new Item 1.05 even if there are doubts as to the critical nature of the relevant information.

When making a materiality determination, a cybersecurity incident will trigger disclosure under Item 1.05 of Form 8-K based on the traditional materiality standards of whether there is a substantial likelihood that a reasonable shareholder would consider the information important in making an investment decision or the information would have significantly altered the “total mix” of information made available by the company. A materiality determination is not dependent on where the cybersecurity incident occurred or who owns the relevant information technology systems.

When preparing Item 1.05 disclosures, the Form 8-K should describe the material aspects of the nature, scope, and timing of the incident. The Form 8-K should also disclose the impact of the cybersecurity incident considering quantitative and qualitative factors such as the effect on the company's results of operations and financial condition, the impact on its vendor, and customer contracts, reputational harm, and potential litigation.

Once an Item 1.05 Form 8-K is filed, a company should provide any material updates in an amended Form 8-K filing. In what will likely be a very limited exception, a company may delay its Form 8-K filing if the US Attorney General determines immediate disclosure would pose a substantial risk to national security or public safety.

FORM 10-K/CYBERSECURITY RISK MANAGEMENT, STRATEGY, AND GOVERNANCE

New Item 106(b) of Regulation S-K will require companies to disclose in their Annual Report on Form 10-K their processes for assessing, identifying, and managing material risks from cybersecurity threats. When preparing this disclosure, companies should consider the following the nonexclusive list of disclosure items:

- Whether and how any such processes for managing risks from cybersecurity threats 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; and
- Whether the company has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

Additionally, companies will also be required to describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, including with respect to its financial condition, results of operations, and business strategy.

When adding new Item 106(c) of Regulation S-K, the SEC streamlined the governance disclosures from those initially proposed. Companies will not have to disclose any cybersecurity expertise of their directors and instead will focus their disclosures on how the board oversees cybersecurity threat risks, identifying the committee responsible for such oversight, and how the board or committee stays informed about these risks. Companies will also be required to provide disclosures about management's role in assessing and managing material cybersecurity threat risks considering the following nonexclusive factors:

- Whether and which management positions or committees are responsible for assessing and managing such material cybersecurity threat 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 material cybersecurity threat risks to the board of directors or a committee or subcommittee of the board of directors.

TIMELINE FOR IMPLEMENTATION

Item 1.05 of Form 8-K/Cybersecurity Incident Reporting

Companies will be subject to the new Form 8-K requirements starting on 18 December 2023. Smaller reporting companies will be subject to the new Form 8-K requirements starting on 15 June 2024.

Item 106 of Regulation S-K/Cybersecurity Risk Management, Strategy, and Governance

Disclosure is required in Annual Reports on Form 10-K for fiscal years ending on or after 15 December 2023.

WHAT COMPANIES SHOULD DO NOW

To prepare for the new reporting and disclosure requirements under the final rules, companies should take the following steps:

Implement, Review, and Periodically Test Incident Response Plans

Given the SEC's focus on disclosure controls and procedures with respect to cybersecurity incidents, companies should review their procedures for how to handle cybersecurity incidents. As part of implementing or reviewing these procedures, companies should ensure that the information flow between those individuals who identify and investigate cybersecurity incidents and those individuals who speak publicly for the company and prepare its SEC disclosures is frequent and comprehensive. Companies should also make sure to have processes to review on a relatively frequent basis any unauthorized occurrences or series of related unauthorized occurrences to be able to make a materiality determination without unreasonable delay.

Understand Use of Third-Party Service Providers

As noted in the final rules, materiality for a cybersecurity incident "turns on how a reasonable investor would consider the incident's impact on the registrant" and not on whose system the data is stored or who owns the electronic IT system. As a result, companies need to review and assess any third-party service provider's incident response readiness and understand the procedures for notification of a cybersecurity incident. It is also important for companies to review their contractual protections for cybersecurity incidents with their third-party service providers and consider any revisions or changes that may need to be made in light of the final rules.

Evaluate Current Cybersecurity Risk management, Strategy, and Governance

Given the new disclosure requirements in Item 106 of Regulation S-K, companies should consider any improvements to their risk management, strategy, and governance structures in light of the anticipated disclosures. As part of this process, companies should review current board and committee responsibilities, and also the disclosure controls and procedures for cybersecurity incidents. Companies should also consider preparing mock-up disclosures for the new Item 106 requirements well in advance of their Form 10-K reporting cycle.

KEY CONTACTS

JULIE F. RIZZO
PARTNER

RALEIGH
+1.919.743.7336
JULIE.RIZZO@KLGATES.COM

TYLER G. ANDERS
ASSOCIATE

NASHVILLE
+1.615.514.1805
TYLER.ANDERS@KLGATES.COM

KYLIE S. HERRING
ASSOCIATE

RALEIGH
+1.919.831.7029
KYLIE.HERRING@KLGATES.COM

