KING & SPALDING
Client Alert

JULY 31, 2023

SEC Adopts Final Cybersecurity Disclosure Rules

For more information, contact:

Elizabeth Morgan
+1 212 556 2351
emorgan@kslaw.com

William Johnson
+1 212 556 2125
wjohnson@kslaw.com

Zachary L. Cochran
+1 404 572 3518
zcochran@kslaw.com

Zachary J. Davis
+1 404 572 2770
zdavis@kslaw.com

King & Spalding

New York
1185 Avenue of the Americas
34th Floor
New York, NY 10036
Tel: +1 212 556 2100

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

On July 26, 2023, the U.S. Securities and Exchange Commission (the "Commission") adopted final rules on cybersecurity risk management, strategy, governance, and incident disclosure by a split vote of 3-2[i]. While the Commission made a number of important changes to the proposed rules, the final rules implement the same basic structure as initially proposed, requiring reporting of material cybersecurity incidents on Form 8-K or Form 6-K, and disclosure of cybersecurity risk management, strategy, and governance in annual reports.

The rules proposed in March 2022 were released following interpretive guidance issued by staff of the Division of Corporation Finance in 2011, and by the Commission in 2018, on the application of existing disclosure requirements to cybersecurity risk and incidents. Although the Commission has observed that registrants' disclosures of material cybersecurity incidents and cybersecurity risk management and governance have improved since the 2011 and 2018 guidance, in the adopting release, the Commission states that they "remain persuaded that…under-disclosure regarding cybersecurity persists despite the Commission's prior guidance" and "investors need more timely and consistent cybersecurity disclosure to make informed investment decisions."

KEY REQUIREMENTS OF THE FINAL RULES

Incident Reporting

The final rules amend Form 8-K to add a new Item 1.05, which will require disclosures of material cybersecurity incidents.

Reporting is required within four business days of materiality determination. Registrants must disclose a material "cybersecurity incident" on Form 8-K within four business days of making the materiality determination. The materiality determination must be made "without unreasonable delay" after discovery of the incident – a less aggressive standard than the proposed requirement of "as soon as reasonably practical."

The rules include a limited delayed disclosure exception for national security and public safety risks. A registrant may delay disclosure of an incident when such disclosure would pose a "substantial risk to national security or public safety." This provision, which was not contemplated by the proposed rules, requires input from the United States Attorney General, who must provide written notice to the Commission of the Attorney General's determination that the incident poses this level of risk. If the Attorney General provides such written notification, the registrant can delay disclosure for up to 120 days, in a series of two 30-day periods and an additional 60-day period (and possibly beyond if the Attorney General requests it).

Form 8-K disclosure requirements focus on the impacts of the incident. If a cybersecurity incident is material, Item 1.05(a) of Form 8-K requires disclosure of the material aspects of the nature, scope, and timing of the incident; and the material impact, or reasonably likely material impact on the registrant, including its financial condition and results of operations. In a shift from the proposed rules, the Commission is focused on disclosure of the impacts of the incident on the registrant, not on the details of incident itself. The final rules do not require disclosure of the status of remediation of an incident, whether an incident is ongoing, whether data was compromised, specific or technical information about the planned response to an incident or cybersecurity systems, related networks, or devices, or potential system vulnerabilities in such detail that would impede the response or remediation.

Updated incident disclosure is required on Form 8-K/A. If information required to be disclosed under Item 1.05 of Form 8-K is not determined or unavailable at the time of the initial filing, registrants are required to note this in the initial Form 8-K and file an amendment to the Form 8-K within four business days of the information being determined or becoming available. Other than with respect to such previously undetermined or unavailable information, the final rules do not create a specific requirement to provide updated information relating to a cybersecurity incident. However, the Commission notes in the adopting release that registrants may have a duty to correct or update prior disclosure that becomes materially inaccurate.

A "cybersecurity incident" includes a series of related occurrences. The final rules did not adopt the proposed requirement to disclose a series of previously undisclosed individually immaterial incidents that had become material in the aggregate, instead extending the definition of "cybersecurity incident" to include a "series of related unauthorized occurrences."

Risk Management, Strategy, and Governance Disclosures

The new risk management, strategy, and governance disclosures will be required in annual reports on Form 10-K or 20-F (as opposed to proxy statements).

Risk management and strategy

Under the final rules, a registrant must describe its 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(b) of Regulation S-K includes the following non-exclusive list of disclosure items to be addressed, as applicable:

- whether and how such processes have been integrated into the registrant's overall risk management system or processes;
- whether the registrant engages assessors, consultants, auditors, or other third-parties in connection with such processes; and
- whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.

Registrants must also describe whether any risks from cybersecurity threats, including risks resulting from any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition, and if so, how.

Governance

Under the final rules, registrants must also describe the board of directors' oversight of risks from cybersecurity threats. This disclosure must include, if applicable:

- identification of any board committee or subcommittee responsible for the oversight of such risks; and
- a description of the processes by which the board or such committee is informed about such risks.

Registrants must also describe management's role in assessing and managing material risks from cybersecurity threats. Item 106(c) of Regulation S-K includes the following non-exclusive list of disclosure items to be addressed, as applicable:

- whether and which management positions and committees are responsible for assessing and managing cybersecurity risks;
- 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 or a committee or subcommittee of the board.

Notably, the Commission did not adopt the proposed requirement to disclose board cybersecurity expertise. The governance disclosure provisions also do not require disclosure of the frequency of management and board discussions regarding cybersecurity risks, which had been contemplated by the proposed rules.

FOREIGN PRIVATE ISSUERS

For foreign private issuers, Form 6-K will be amended to require registrants 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 will be updated to require foreign private issuers to make periodic disclosure comparable to the disclosures required in new Regulation S-K Item 106.

TIMELINE FOR COMPLIANCE

Compliance with the Form 8-K and Form 6-K cybersecurity incident disclosure requirements will be required for all registrants other than smaller reporting companies beginning on the later of 90 days after the date of publication in the Federal Register or December 18, 2023; compliance by smaller reporting companies will be required on the later of 270 days after the date of publication in the Federal Register or June 15, 2024. All registrants will be required to include the risk management, strategy, and governance disclosures set forth in Item 106 of Regulation S-K (and the comparable requirements in Form 20-F) in annual reports beginning with fiscal years ending on or after December 15, 2023. For all registrants, inline XBRL tagging will be required one year after initial compliance with the related disclosure requirement.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,300 lawyers in 23 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE
ATLANTA	CHICAGO	GENEVA	MIAMI	RIYADH	TOKYO
AUSTIN	DENVER	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
BRUSSELS	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	

[i] The fact sheet for the final rules can be found here and the adopting release for the final rules can be found here.