Alert

July 27, 2023

COZEN O'CONNOR

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

On July 26, 2023, the Securities and Exchange Commission (SEC) announced the adoption of final rules relating to cybersecurity risk management, strategy, governance, and incident disclosures. The new rules define a cybersecurity incident 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" and requires:

- current disclosure on Form 8-K, of material cybersecurity incidents; and
- periodic disclosure on Form 10-K or Form 20-F, as applicable, of material information regarding cybersecurity risk management, strategy, and governance.

Registrants are required to tag disclosures under the new rules in inline XBRL.

Disclosure of Material Cybersecurity Incidents

The final rules add a new Item 1.05 to Form 8-K that requires registrants to disclose, within four business days after the registrant determines that it has experienced a material cybersecurity incident, the following:

- the material aspects of the cybersecurity incident including the nature, scope, and timing of the cybersecurity incident; and
- the material impact, or reasonably likely material impact, of the cybersecurity incident on the registrant, including such impact on its financial condition and results of operations.

Since the focus of the disclosure is on the material impact of an incident, the instructions to new Item 1.05 provide that "a registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident." In addition, in assessing the material impact of an incident, harm to a registrant's financial condition, and results of operations is not exclusive; in other words, other material impacts could include, for example, harm to a registrant's "reputation, customer or vendor relationships or competitiveness."

Since the timing of the disclosure under new Item 1.05 is triggered by a registrant's determination that it has experienced a material cybersecurity incident, the instructions to new Item 1.05 provide that such materiality determination regarding a cybersecurity incident "must be made without unreasonable delay after discovery of the incident." To the extent information required under Item 1.05 is unavailable at the time of filing the Form 8-K, a registrant is required to include a statement to that effect and must then file an amendment to the Form 8-K within four business days after the registrant, without unreasonable delay, determines such information is available. The only permitted delay to the required disclosures is when the disclosure "poses a substantial risk to national security or public safety" and the U.S. Attorney General has notified the SEC in writing of such determination. A late filing under new Item 1.05 will not, however, result in the loss of Form S-3 eligibility.

Katayun I. Jaffari

Chair, Corporate Governance
Co-Chair, Capital Markets & Securities
Chair, ESG

kjaffari@cozen.com
Phone: (215) 665-4622
Fax: (215) 665-2013

Kevin Roggow

Member

kroggow@cozen.com
Phone: (212) 908-1294
Fax: (212) 509-9492

Rikisha Collins

Associate

rcollins@cozen.com
Phone: (215) 366-4464
Fax: (215) 665-2013

Andrew Baer

Chair, Technology, Privacy & Data Security

abaer@cozen.com
Phone: (215) 665-2185
Fax: (215) 372-2400

It is important to highlight that based on the definition of cybersecurity incident, an incident that occurs on a third-party system that a registrant uses may also require disclosure by the registrant based on the information available to them.

For registrants that are foreign private issuers, amendments have been made to Form 6-K requiring that they furnish information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange or to security holders.

Disclosure of Cybersecurity Risk Management, Strategy, and Governance

The final rules also add a new Item 106 to Regulation S-K as well as corresponding amendments to Form 20-F that require registrants to provide more consistent and informative disclosure on an annual basis regarding the registrant's cybersecurity risk management, strategy, and governance. Under the new Item 106 of Regulation S-K, registrants are required to describe the following:

- their companies' processes for assessing, identifying and managing material risks from cybersecurity threats, in sufficient detail for a reasonable investor to understand such processes, addressing, as applicable, the following non-exhaustive list: (i) whether and how any such processes have been integrated into the registrant's overall risk management system or processes; (ii) whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and (iii) whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider;
- whether any risks from cybersecurity threats 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;
- the registrant's board of directors oversight of risks from cybersecurity threats; and
- the role of management in assessing and managing material risks from cybersecurity threats, addressing, as applicable, the following non-exclusive list: (i) whether and which management positions or committees are responsible for assessing and managing cybersecurity risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise; (ii) the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and (iii) whether such persons or committees report information about such risks to the board of directors or relevant committee or subcommittee of the board of directors.

Timing

Registrants are required to comply with the Form 8-K or Form 6-K, as applicable, material cybersecurity incident disclosure starting on the later of (i) 90 days after the date of publication of the final rules in the Federal Register or (ii) December 18, 2023. Smaller reporting companies are required to comply with the Form 8-K disclosure requirements starting the later of (i) 270 days after the date of publication of the final rules in the Federal Register or (ii) June 15, 2024.

Registrants are also required to include the new annual disclosure regarding cybersecurity risk management, strategy, and governance in annual reports for fiscal years ending on or after December 15, 2023. For calendar year end companies, this will be the Form 10-K or Form 20-F, as applicable, for the 2023 fiscal year.

Takeaways

While the final rules deal specifically with cybersecurity disclosure requirements, other laws and regulations require companies in possession of personal information and/or other sensitive corporate information, or which provide critical infrastructure in supply chains, to implement a risk-based written cybersecurity program that is regularly evaluated, tested, and updated in light of the nature, amount, and sensitivity of data processed by the company, the potential impact of a cybersecurity incident, and the evolving threat environment, among other factors. Best practices also dictate (and the four business day reporting requirement in the final rules effectively requires) that companies implement and periodically test a cybersecurity incident response plan to ensure that the proper stakeholders (including in-house and outside counsel) can be immediately engaged to manage the investigation, mitigation, legal and regulatory compliance, and public disclosure

Matthew J. Siegel, CIPP/US

Member

msiegel@cozen.com
Phone: (215) 665-3703
Fax: (215) 701-2303

Related Practice Areas

- Business
- Capital Markets & Securities
- Corporate
- Technology, Privacy & Data Security

surrounding a cybersecurity incident in order to limit further harm to the company and affected third parties and to preserve legal privilege to the greatest extent possible.

Cozen O'Connor's multidisciplinary Technology, Privacy & Data Security practice group can assist with preparation of best practices, as well as provide crisis management and compliance counseling in the event of an actual cybersecurity incident.