SEC Adopts New Cybersecurity Rules for Issuers

July 27, 2023

On July 26, 2023, the SEC adopted the long-anticipated final rules on cybersecurity risk management, strategy, governance, and incident disclosure for issuers. The new rules are part of the SEC's larger efforts focused on cybersecurity regulation with a growing universe of rules aimed at different types of SEC registrants, including: (i) its proposed cybersecurity rules for registered investment advisers and funds and market entities, including broker-dealers, (ii) its proposed amendments to Reg S-P and Reg SCI and (iii) existing cybersecurity obligations under SEC regulations, including Reg S-P, Reg S-ID, and the recently amended Form PF.

KEY REQUIREMENTS

The rules introduce three new types of disclosure requirements relating to: (1) material cybersecurity incidents, (2) cybersecurity risk management processes and (3) cybersecurity management and governance.

- **Current Disclosure of Material Cybersecurity Incidents**. The rules require registrants to disclose certain information about a material cybersecurity incident under new Item 1.05 of Form 8-K ("Item 1.05") within four business days of determining that a cybersecurity incident it has experienced is material. The determination of materiality is to be made "without unreasonable delay," as opposed to "as soon as reasonably practical" as was proposed.

    - *Materiality Analysis:* The final rules revise the materiality analysis in the proposed rules, and require disclosure of the material aspects of the nature, scope, timing of the incident and the material impact or reasonably likely material impact of the incident on the registrant (including its financial condition and results of operations), to the extent the information is known at the time of the Form 8-K filing. 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.

- *Form 8-K Amendment:* Notably, to the extent any required information is not determined or is unavailable at the time of the required filing, registrants are required to include a statement to this effect in the Form 8-K and then file a Form 8-K amendment containing such information within four business days after the registrant determines such information or within four business days after such information becomes available. This is a departure from the proposed rules that would have required registrants to update incident disclosures in Forms 10-K or 10-Q.

- *Series of Related Unauthorized Occurrences*: The rules adopt a definition of "cybersecurity incident" that extends to "a series of related unauthorized occurrences." Accordingly, if a registrant determines that it has been materially affected by a series of related cyber intrusions, Item 1.05 may be triggered even if the material impact or reasonably likely material impact of each individual intrusion is by itself immaterial. This replaces the proposed rule which would have required disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents became material in the aggregate.

- *National Security and Public Safety Delay Provision:* The final rules introduce a very narrow national security and public safety delay provision, such that disclosure of a cybersecurity incident may be delayed, initially for up to 30 days, if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. Two subsequent delay periods of 30 days and 60 days (in extraordinary circumstances) each may be sought in a similar fashion. If the Attorney General indicates that further delay is necessary beyond the final 60-day delay, the Commission will consider additional requests for delay and may grant such delay through a Commission exemptive order.

- *Foreign Private Issuers*: The rules amend Form 6-K to require foreign private issuers ("FPIs") that are required to furnish such reports, to disclose on Form 6-K material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange or to security holders, promptly after the material contained in the report is made public.

- *Safe Harbors:* Consistent with the proposed rules, the final rules provide for certain limited safe harbors, including from liability under Exchange Act

Section 10(b) and Rule 10b-5 thereunder and protection against loss of Form S-3 eligibility, in each case for filing failures related to Item 1.05 of Form 8-K.

A comparison of the final version of Item 1.05 of Form 8-K with the proposed version is here.

- **Periodic Disclosure of Cybersecurity Risk Management Processes**. Registrants will be required to make several disclosures related to cybersecurity risk management programs in their Forms 10-K and 10-Q, including whether and how registrants assess, identify and manage material risks, whether the registrant engages any third-parties, auditors or consultants in connection with such processes and whether the registrant has processes in place to oversee and identify third-party risk, which represents a more streamlined disclosure requirement when compared to the rules as proposed. Notably, the final rules substitute disclosure of "policies and procedures" for the term "processes," which the SEC believes more fully encompasses registrants' cybersecurity practices. Registrants will need to describe whether any risks for cybersecurity threats, current or previous, have materially affected or are likely to materially affect business strategy, operations or financial conditions. Parallel requirements apply to FPIs in respect of their Form 20-F filings.

- **Cybersecurity Management & Governance**. Registrants, including FPIs, will be required to describe the board's oversight of and management's role in assessing and managing risks posed by cybersecurity threats in their Forms 10-K, 10-Q and 20-F, as applicable. The final rules streamline the enumerated disclosure elements initially proposed. With respect to management's role, registrants must address, to the extent applicable, which management positions or subcommittees are responsible for assessing and managing such risks, including the relevant expertise of such persons; the process by which management or their committees are informed about and monitor the prevention, detection, mitigation and remediation of cybersecurity incidents and whether such person or committees report information about such risks to the board or a subcommittee of the board. Registrants are required to disclose whether members of management have prior work experience, education, or knowledge, skills or other background in cybersecurity; to the extent they are involved in cybersecurity risk management. This is a departure from the proposed rules, which would have required similar information in respect of directors. If applicable, registrants will be required to identify the board committee or subcommittee responsible for overseeing cybersecurity risks and describe the process by which they are informed of cybersecurity risks.

- **Effective Date**. With respect to Item 1.05 and the new Form 6-K requirements, registrants other than small reporting companies must begin complying on the later

of 90 days after the date of publication or December 18, 2023. Smaller reporting companies will 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. With respect to the disclosures required in Form 10-Q and 10-K and the comparable requirements in Form 20-F, registrants must provide disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. Inline XBRL tagging must begin one year after initial compliance with the related disclosure requirement.

The final rules are available here.

We will publish a more detailed analysis of the impact of the new rules in the coming weeks.

To subscribe to the Data Blog of our Data Strategy and Security practice, please click here.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK


Charu A. Chandrasekhar
cachandrasekhar@debevoise.com


Avi Gesser
agesser@debevoise.com


Matthew E. Kaplan
mekaplan@debevoise.com


Erez Liebermann
eliebermann@debevoise.com

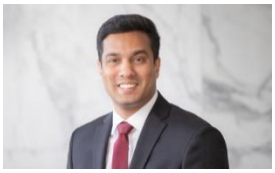

Benjamin R. Pedersen
brpedersen@debevoise.com


Paul M. Rodel
pmrodel@debevoise.com


Steven J. Slutzky
sjslutzky@debevoise.com


Matt Kelly
makelly@debevoise.com


Kelly Donoghue
kgdonoghue@debevoise.com


John Jacob
jjacob@debevoise.com


Amy Pereira
apereira@debevoise.com


Chris Duff
ceduff@debevoise.com

WASHINGTON, D.C.


Luke Dembosky
ldembosky@debevoise.com

SAN FRANCISCO


Mengyi Xi
mxu@debevoise.com