Simpson Thacher

Regulatory and Enforcement Alert

SEC Adopts Final Rules For Public Companies Relating to Cyber Incident Disclosure and Cybersecurity Risk Management, Strategy and Governance Matters

July 27, 2023

On July 26, 2023, by a divided 3-2 vote, the SEC approved final rules relating to cybersecurity risk management, strategy, governance and incident disclosure (the "Final Rule"),[1] amending the rule first proposed in March 2022 (the "Proposed Rule").[2]

The Final Rule, which will become effective 30 days after publication in the Federal Register, will apply to all public companies subject to the reporting requirements of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), including foreign private issuers, smaller reporting companies and business development companies, and will require current reporting on Form 8-K of material cybersecurity incidents and periodic reporting on Form 10-K of existing policies and procedures to identify and manage cybersecurity risk, including the role of management and the board of directors in cybersecurity risk management and oversight.

While public company issuers were already subject to two sets of guidance requiring the disclosure of material cybersecurity risks and incidents in various sections of their periodic reports,[3] the Final Rule imposes a short time period to report material cybersecurity incidents in current 8-K reporting and also significantly expands the required discussion of cybersecurity risk management and oversight in a company's Form 10-K or 20-F, as applicable.

The Final Rule generally tracks the earlier Proposed Rule, but there are several notable changes, including:

- Slightly narrowing the scope of the contemplated required Form 8-K disclosure for material cybersecurity incidents;
- Adding a limited delay option to the Form 8-K requirement for material cybersecurity incidents where disclosure would implicate national security or public safety concerns;

[1] See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure as well as Public Company Cybersecurity Fact Sheet.

[2] See Proposed Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rules as well as Proposed Rule Public Company Cybersecurity Fact Sheet.

[3] CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011) and Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 26, 2018) No. 33-10459 (Feb. 21, 2018) [83 FR 8166].

- Removing the proposed Form 10-K or Form 10-Q requirement to disclose previously undisclosed individually immaterial cybersecurity incidents that become material in the aggregate and instead:
  - Requiring amendments to prior Form 8-K disclosure of cybersecurity incidents for information not determined or available at the time of initial filing; and
  - Defining the term "cybersecurity incident" to include a series of related unauthorized occurrences, to reflect the fact that cyberattacks can compound over time.
- Deleting the contemplated requirement to disclose board cybersecurity expertise.

Summary: Requirements of the Final Rule

Form	Rule	Requirements
8-K	Item 1.05–*Material Cybersecurity Incidents*	Registrants must disclose any cybersecurity incident that is determined to be material within four business days of that determination, and describe the material aspects of its: • Nature, scope, and timing; and • Impact or reasonably likely impact on the registrant, including its financial condition and results of operations. In cases where the U.S. Attorney General determines that disclosure on this timeline would pose a substantial risk to national security or public safety, the Form 8-K may be delayed for 30 days (or more).
10-K or 20F	Item 106(b) of Regulation S-K–*Risk Management and Strategy* Item 16K of Form 20-F–*Cybersecurity*	Registrants must: • Describe their processes for 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.

10-K or 20-F	Item 106(c) of Regulation S-K– *Governance* Item 16K of Form 20-F– *Cybersecurity*	Registrants must: • Describe the board's oversight of risks from cybersecurity threats, including any specific board committee or subcommittee tasked with oversight of cybersecurity risks. • Describe management's role in assessing and managing material risks from cybersecurity threats, including: ◦ Whether and which management positions or committees are responsible for assessing and managing such risks and the relevant expertise of such persons; ◦ 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 board committee or subcommittee.
6-K	-	Foreign Private Issuers must furnish information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders.

Compliance Dates

Form	Rule	Date
10-K/20-F	Item 106 of Regulation S-K/Item 16K	Beginning with annual reports for fiscal years ending on or after December 15, 2023. In addition, all registrants must begin tagging responsive disclosure in Inline XBRL beginning with annual reports for fiscal years ending on or after December 15, 2024.
8-K/6-K	Item 1.05	For all registrants other than smaller reporting companies, 90 days after date of publication in the Federal Register or December 18, 2023, whichever is later. Smaller reporting companies must begin compliance 270 days after date of publication in the Federal Register or June 15, 2024, whichever is later. In addition, all registrants must begin tagging responsive disclosure in Inline XBRL beginning on December 18, 2024 or 465 days after the date of publication of the Final Rule in the Federal Register, whichever is later.

Discussion of Key Elements and Changes from Proposed Rule: Current Reporting Items

TIMELY REPORTING OF MATERIAL CYBERSECURITY INCIDENTS

The Final Rule requires that registrants disclose information about a cybersecurity incident within four business days after the registrant determines that the cybersecurity incident is material. Importantly, registrants are not required to start this four business day disclosure clock on the date of the incident itself. The instruction to Item 1.05 notes that the materiality determination must be made "without unreasonable delay," and the SEC's adopting release for the Final Rule (the "Adopting Release") also points out a change from the proposed language requiring a determination "as soon as reasonably practicable." This change was meant to alleviate undue pressure on issuers to make materiality determinations on an inappropriately accelerated timeline.

With respect to determinations of materiality, the SEC clarified in the Adopting Release that the determination is meant to be made in accordance with the prevailing and familiar definition of materiality: information is material

if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available."[4]

The Final Rule added a limited exception to the four business day 8-K disclosure requirement in the event that the incident is determined by the United States Attorney General to pose a risk to national security or public safety. In practice, this will likely require an instruction from the Department of Justice to an issuer that it is concerned that public disclosure might risk national security or public safety interests. In these instances, registrants may delay disclosure by 30 days (or longer, if the Attorney General determines that the risk is ongoing). The ability to make use of the exception, or complete a timely filing, if the exception is not granted, will put issuers at the mercy of prompt decision-making and interagency communication. The Adopting Release notes that the SEC has consulted with the Department of Justice to establish an interagency communication process, but the limits of the 8-K reporting timeline will put pressure on that process and could limit the utility of the exception.

The Final Rule, similar to the Proposed Rule, provides that the untimely filing of an 8-K under new Item 1.05 will not result in the loss of Form S-3 eligibility.

DISCLOSURE OF THE NATURE AND SCOPE OF A CYBERSECURITY INCIDENT

The Final Rule requires that registrants disclose the nature, scope, and timing of a material cybersecurity incident, as well as the impact or reasonably likely impact on the registrant's business. This represents a slight narrowing from the Proposed Rule, which had required that registrants also disclose specific information about when the incident was discovered, whether it was ongoing and whether any data was stolen, altered, accessed or used for any other unauthorized purpose. Commenters stated that this information was too specific for registrants to compile quickly and that disclosing the information could open up registrants to additional risks. The SEC amended the Final Rule to include only general details about the incident and its likely impact.

8-K AMENDMENT FOR PREVIOUSLY UNAVAILABLE INFORMATION

The Final Rule provides that, to the extent information required to be disclosed in an Item 1.05 8-K is not determined or is unavailable at the time of the required filing, the registrant must include a statement to this effect in the initial filing and must disclose such information in an amendment to the Form 8-K within four business days after the registrant, without unreasonable delay, determines such information or such information becomes available. In contrast, the Proposed Rule had contemplated that registrants would update disclosure relating to previously disclosed cybersecurity incidents in its subsequent 10-Q or 10-K filings. The Adopting Release notes that requiring such disclosure in an 8-K amendment, rather than in a periodic report, is intended to enable investors to more quickly and easily identify updates regarding previously disclosed incidents.

[4] *TSC Indus. v. Northway*, 426 U.S. 438, 449 (1976).

Discussion of Key Elements and Changes from Proposed Rule: Periodic Reporting Items

CYBERSECURITY EXPERTISE OF MANAGEMENT

The Final Rule requires that registrants disclose information about cybersecurity governance, including the board of directors' oversight role regarding cybersecurity risks and management's role and relevant expertise in assessing and managing cybersecurity related risks and implementing related policies, procedures and strategies.

Notably, the Proposed Rule had also required that registrants disclose whether any member of the board of directors had cybersecurity expertise. Commenters stated concerns that it may not be practical for a board to recruit dedicated cybersecurity experts, given the small size of most boards and other practical considerations around public company board service. The SEC amended the Final Rule to eliminate this disclosure requirement. The Final Rule still requires that a registrant disclose management's relevant cybersecurity expertise, which certain of the Commissioners noted during the SEC's Open Meeting is a requirement that does not apply to other areas of key risk within a company.

New SEC Definitions for Cybersecurity Incident, Cybersecurity Threat and Information Systems

In Item 106(a) of Regulation S-K, "cybersecurity incident," "cybersecurity threat," and "information systems" are defined as follows:

- "Cybersecurity incident" means "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."
- "Cybersecurity threat" means "any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."
- "Information systems" means "electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations."

The SEC minimally altered the above three definitions from the Proposed Rule. The most notable change appears in the definition of "cybersecurity incident," where the SEC clarified that "a series of related unauthorized occurrences" falls within the definition. This definition shift expands the coverage of disclosure requirements in Item 1.05 of Form 8-K.

Next Steps for Issuers to Consider

With the adoption of the Final Rule, the SEC has emphasized the need for investors to have access to consistent, easily locatable, and timely information related to what the SEC has described as a key risk facing companies and their investors. For public company issuers, the near-term focus should be on:

- Ensuring appropriate incident reporting and elevation practices are in place to evaluate, address and remediate incidents, adding in the necessary processes to determine whether and when an incident is material such that it requires timely disclosure;
- Re-evaluating the governance and cyber risk mitigation practices to ensure that they adequately address the risks the company faces; and
- Reviewing existing cybersecurity governance and risk management disclosures to identify updates that may be required in the issuer's next Form 10-K or 20-F, as applicable.

For further information regarding this Alert, please contact one of the following authors:

NEW YORK CITY

Marc P. Berger
+1-212-455-2197
marc.berger@stblaw.com

Karen Hsu Kelley
+1-212-455-2408
kkelley@stblaw.com

Leah Malone
+1-212-455-3560
leah.malone@stblaw.com

Courtney Kobren
+1-212-455-7026
courtney.kobren@stblaw.com

Jessica N. Cohen
+1-212-455-7736
jessica.cohen@stblaw.com

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Charles Mathes
+1-212-455-2258
charles.mathes@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Joshua A. Levine
+1-212-455-7694
jlevine@stblaw.com

Michael J. Osnato, Jr.
+1-212-455-3252
michael.osnato@stblaw.com

WASHINGTON, D.C.

Jeffrey H. Knox
+1-202-636-5532
jeffrey.knox@stblaw.com