wiley

ALERT

SEC Adopts Controversial New Cybersecurity Disclosure Rules for Public Companies

August 1, 2023

Public companies will soon face new cybersecurity disclosure requirements from the Securities and Exchange Commission (SEC), which voted last week to approve a controversial new cybersecurity rule. The final rule—which is part of an increasing number of reporting and disclosure requirements the federal government is issuing to mandate disclosure of cybersecurity incidents—will impose a variety of new public disclosure requirements on publicly traded companies. The agency says the rule is designed to keep investors informed about a company's material cybersecurity incidents and its cybersecurity risk management, strategy, and governance mechanisms.

The new SEC requirements—which have different roll-out dates—will create additional compliance burdens on public companies, many of whom are already subject to various other cyber incident reporting and regulatory obligations. With the growing patchwork of cybersecurity and incident reporting requirements at both the federal and state levels—it is more important than ever to understand these complex rules. In the context of multiplying mandates, and risk related to shareholder class actions, the SEC's decision to proceed with its own rules presents challenges to public companies.

Overview of the SEC's New Cybersecurity Incident Disclosure Rule

On July 26, 2023, the SEC voted 3-2 to approve the final rule in its Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure proceeding. As background, the SEC previewed this rule with its March 2022 Notice of Proposed Rulemaking (NPRM). In response to the NPRM, the SEC received over 150 comments, many of which were critical of key elements of the proposal as well as the

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
jfbrown@wiley.law

Boyd Garriott
Associate
202.719.4487
bgarriott@wiley.law

Jillian M. Quigley
Associate
202.719.4668
jquigley@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
Securities Enforcement and Litigation
Telecom, Media & Technology

need for new rules given the myriad other cyber obligations faced by diverse public companies.

The SEC made a number of changes between the NPRM and the final rule, such as purporting to narrow the type and amount of information required to be disclosed, and providing for a very narrow option to seek a determination by the Attorney General of the United States that a delay in disclosure is needed to address a substantial risk to national security or public safety.[1] In large part, the final rule is structured similarly to the proposed rule, requiring:

- Disclosure of a material cybersecurity incident within 4 business days on Form 8-K; and
- Disclosure of cyber risk management, strategy, and governance on Form 10-K.

The SEC explains that the impetus behind this rule is the economy's increasing dependence "on electronic systems, such that disruptions to those systems can have significant effects on registrants,"[2] and the rise in major cybersecurity incidents in recent years. The Commission further notes that although existing guidance confirms the need to disclose information about material events and cyber risks, there are no specific guidelines for where or how companies are supposed to report cybersecurity incidents in SEC filings, which it claims makes it "difficult for investors to locate, interpret, and analyze the information provided."[3]

Key Deadlines

Overall, the rule will become effective 30 days after Federal Register publication, but the SEC lays out additional timelines for the various requirements within the rule. Specifically:

- The requirement to describe the company's cyber risk management, strategy, and governance will be effective December 15, 2023.
- The incident disclosure requirement will be effective the latter of: (1) December 18, 2023; or (2) 90 days after Federal Register publication.
    - Smaller companies must comply with the incident disclosure requirement the latter of: (1) June 15, 2024; or (2) 270 days after Federal Register publication.

Summary of New Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

New Requirement to Disclose Material Cybersecurity Incidents within 4 Business Days on Form 8-K. In line with its proposed rule, the SEC officially adopted and designated Item 1.05 of Form 8-K as the main mechanism through which companies must comply with cyber incident reporting obligations. The new rule will amend Form 8-K to require registrants to disclose any cybersecurity incident that is considered material and to describe the: (1) material aspects of its nature, scope, and timing of the incident; and (2) material impact or reasonably likely material impact of the incident which may vary from incident to incident, including but not limited to financial condition and results of operations.[4]

The rule provides additional guidance and parameters around this new requirement:

- ***Companies Must Report Cybersecurity Incidents that Are "Material."*** The SEC limits disclosure reporting obligations to cybersecurity incidents that are *material* in nature. Numerous commenters urged the SEC to provide clarity about materiality determinations. "Material" is described in the final rule as reflecting "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 available."[5] In describing the bounds of what should be considered a material incident, the SEC explains that companies should consider both quantitative *and* qualitative factors in assessing the material impact of an incident, including non-tangible effects such as harm to a company's reputation, customer or vendor relationships, or competitiveness.[6] The possibility of litigation or regulatory investigations or actions may also constitute a reasonably likely material impact on the registrant.[7] Of note, the final rule does not include a quantitative threshold that triggers disclosure because, as the SEC explains, there are numerous non-quantifiable indicia that may make an incident material such as future or current harm to a company's reputation, customers, or other parties.[8]
- ***Disclosure Must Be Made Four Business Days After Materiality Determination.*** An Item 1.05 disclosure must be filed within four business days of determining that an incident is material.[9] Numerous commenters raised concerns about the short timeline and suggested that the agency permit companies to wait until an incident has been contained or remediated, or to allow delays when there is an active law enforcement investigation. Many commenters questioned how unreasonably short deadlines would affect a company's ability to appropriately mitigate, contain, remediate, or otherwise address the incident. Despite this, the SEC concluded that the four-day timeline was reasonable and declined to extend it any further,[10] subject to the extremely limited Attorney General delay provision discussed below.
- ***Materiality Determinations Must Be Made "Without Unreasonable Delay".*** The final rule also addresses the speed with which a company must make a materiality determination after discovery of an incident. The SEC originally proposed in the NPRM an instruction that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."[11] The SEC revised the instruction to require companies to make their materiality determinations "without unreasonable delay."[12] The SEC recognized that a materiality determination necessitates an informed and deliberative process which cannot be rushed prematurely nor unreasonably delayed in an effort to avoid timely disclosure.[13] At the same time, the SEC also warned companies not to change their policies to encourage delays.[14]
- ***Proposed Item 106(d)(1) Replaced by New Instructions in Form 8-K.*** The SEC declines to adopt proposed Item 106(d)(1) and instead issues a new instruction to clarify that updated incident disclosure must be provided in a Form 8-K amendment.[15] Registrants must now submit an amended Form 8-K to supplement the record with any information required under Item 1.05(a) of Form 8-K that could not be provided initially.[16]
- ***No Continuing Duty to Update Prior Statement.*** The final rule will not create a continuing duty to update prior statements, but the SEC did remind entities that they may have a duty to cure prior disclosures to the extent that information provided therein turns out to have been untrue or

misleading,[17] including by omission.

- ***U.S. Attorney General Can Delay Disclosures Due To Substantial Risk To National Security or Public Safety.*** Commenters expressed concern that early public disclosures will undermine criminal and other investigations. The final rule purports to address this concern with a narrow solution that appears impractical. It adopts a provision that allows a registrant to delay disclosure for up to 30 days from the normal disclosure deadline but only where "the Attorney General determines that the disclosure poses a substantial risk to national security or public safety and notifies the Commission of such determination in writing."[18] Delays may be extended for an additional 30 days (*i.e.*, up to 60 days after the normal disclosure deadline) where "the Attorney General determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing."[19] In extraordinary circumstances, the SEC will allow an additional 60-day delay where disclosure "continues to pose a substantial risk to national security" and the Attorney General notifies the Commission accordingly.[20] Notably, there is no provision for the Director of National Intelligence (DNI) who oversees the U.S. Intelligence Community, the Secretary of Defense who serves as the President's principal advisor on national defense, or the Director of the Cybersecurity and Infrastructure Security Agency (CISA) which acts as the nation's cyber defense agency or other federal agencies to seek a disclosure delay. Moreover, federal and non-federal agencies are not precluded from requesting the Attorney General to notify the SEC of a disclosure delay.[21]
- ***Item 1.05 From Form 8-K Must Be Filed.*** In the final rule, the SEC declines to permit registrants to furnish, rather than file, Item 1.05 Form 8-K to "promote the accuracy and reliability of such disclosures for the benefit of investors."[22]
- ***No Ban on Insider Trading During Materiality Determination Period.*** The SEC also declines to adopt a ban on trading by insiders during the materiality determination time period. Even though there is no mandated time period within which a materiality determination must be made, the SEC suggests that "the risk of insider trading is low given the limited time period between experiencing a material incident and public disclosure."[23] The Commission does go on to note, however, that recent amendments to 17 CFR 240.10b5-1 (Rule 10b5-1), the provision that provides an affirmative defense to insider trading liability for directors and officers, now requires officers and directors to certify that at the time they adopted a trading plan they were unaware of material nonpublic information about the issuer or its securities and adopted the plan in good faith.[24] The SEC believes this will provide sufficient coverage to alleviate concerns about insider trading during the interim period between incident discovery and an associated 8-K filing. [25]
- ***Delayed Reporting Permitted Where There Is Conflict with FCC's CPNI Rules.*** The SEC concedes that there was a conflict between the its disclosure rules and the Federal Communications Commission's (FCC) customer proprietary network information (CPNI) rule requiring entities to refrain from notifying customers or disclosing a breach publicly until seven business days have passed following the notification to the U.S. Secret Service (USSS) and Federal Bureau of Investigation (FBI).[26] To resolve the conflict with the FCC's CPNI rules, entities that are subject to the CPNI rule can delay an 8-K filing up to seven business days following notification to USSS and the FBI upon written notification to the

SEC.[27] The SEC otherwise concluded that Item 1.05 neither directly conflicts with nor impedes other federal laws or regulations.[28]

- ***Other Cybersecurity Incident Reporting Obligations Not Factored into Reporting Timeline to SEC.*** Throughout the robust record, a common theme was the need for harmonization between the SEC's rules and the growing patchwork of other cybersecurity incident reporting requirements—both at the federal level and across the states. However, the SEC's final rule does not account for these other obligations, finding instead that because rules have different goals, the SEC is justified in proceeding to require public disclosures within four days. With respect to the Cyber Incident Reporting for Critical Infrastructure Act of 2023 (CIRCIA) and CISA's forthcoming implementing regulations, the SEC argues that the two serve different purposes,[29] and finds it unlikely that the CIRCIA regulations would affect the balance of material information available to investors about public companies because the CIRCIA reporting regime is confidential.[30] And to the extent that state privacy or insurance laws excuse or permit entities to delay notification of cyber incidents, the SEC will still require entities to timely disclose such incidents in Form 8-K. The SEC appears not to be troubled that its rules may upset carefully constructed approaches by CISA, states and other agencies with respect to confidential handling of information and cooperation.

New Requirements to Disclose Cyber Risk Management, Strategy, and Governance. In addition to the cyber incident reporting disclosures, the new rules impose other periodic disclosure requirements about cybersecurity risk management, strategy, and governance.

- ***General Cyber Risk Management Disclosures Required.*** As adopted, Regulation S-K, Item 106(b)(1) requires a description of "the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes."[31] The SEC expects the disclosure will allow investors to ascertain a registrant's cybersecurity practices, such as whether they have a risk assessment program in place, with sufficient detail for investors to understand the registrant's cybersecurity risk profile. [32] Of note, the SEC added a materiality qualifier to the proposed requirement to disclose "risks from cybersecurity threats" but removed the proposed list of risk types (*e.g.,* "intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk") to avoid being seen as prescribing cybersecurity policy.[33] The SEC also revised Item 106(b)'s enumerated disclosure elements to require only high-level disclosure regarding third-party service providers.[34] The final rules will require disclosures about whether registrants engage assessors, consultants, auditors, or other third parties in connection with their cybersecurity (although registrants are not required to name the third parties).[35]
- ***Corporate Governance Disclosures Required.*** The final rule modifies proposed Item 106(c) of Regulation S-K, which now requires registrants to: (1) Describe the board's oversight of risks from cybersecurity threats;[36] and (2) Describe management's role in assessing and managing *material* risks from cybersecurity threats including:[37]

  - Whether and which positions or committees are responsible for risk assessment and management and the relevant expertise of people in these roles;
  - The processes through which people or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity risks to the board of directors or a committee or subcommittee thereof;
  - Whether those involved in the aforementioned roles report information about these risks.
- ***Disclosure By Foreign Private Issuers Required.*** With some exceptions, the final rule adopts disclosure requirements for Foreign Private Investors (FPI) that are parallel to those proposed for domestic issuers in Regulation S-K Items 106 and 407(j) and Form 8-K Item 1.05 for material cybersecurity incidents.[38]
- ***Compliance with Structured Data Requirements Delayed for One Year***. The final rule also mandates that registrants tag the new disclosures in Inline XBRL, including by block text tagging narrative disclosures and detail tagging quantitative amounts.[39] Compliance with the structured data requirements will be delayed for one year beyond the initial deadline to comply with the new disclosure requirements.

Effect of the Final Rule on Earlier Guidance. In response to questions about the final rule's effect on the 2011 Staff Guidance and 2018 Interpretive release, the SEC notes that the final rules "supplement the prior guidance but do not replace it."[40] Moreover, many of the issues discussed in the 2018 Interpretive Release are unaddressed by the final rules.[41]

Key Takeaways

The new SEC rules add to the already complex patchwork of cybersecurity incident reporting requirements, and they present a number of operational challenges that public companies will need to work through.

We anticipate these requirements will lead to an increase in whistleblower claims, investigations, and litigation about cyber incidents, including inquiries related to potential insider trading, disclosures about incidents, and disclosures about management.

***

Wiley's Privacy, Cyber & Data Governance Team has helped companies of all sizes from various sectors proactively address risks and address compliance with new cybersecurity laws and requirements. Our team has been actively involved in almost every proceeding that is referenced in the Strategy and is advising clients on the likely results of new legislation, revisions to core NIST documents, and agency regulatory and oversight activities. Please reach out to any of the authors with questions.

[1] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release Nos. 33-11216, 34-97989, File No. S7-09-22, at 28 (July 26, 2023) (Final Rule).

[2] Final Rule at 7.

[3] Final Rule at 6-7.

[4] Final Rule at 29 ("The final rules will require the registrant to 'describe 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.'").

[5] Final Rule at 80.

[6] Final Rule at 29.

[7] Final Rule at 29-30.

[8] Final Rule at 37.

[9] Final Rule at 31-32.

[10] Final Rule at 32-33.

[11] Final Rule at 14.

[12] Final Rule at 37.

[13] Final Rule at 37.

[14] Final Rule at 38.

[15] Final Rule at 51-52.

[16] Final Rule at 51-52.

[17] Final Rule at 51-52.

[18] Final Rule at 34.

[19] Final Rule at 34.

[20] Final Rule at 34-35. This additional 60-day in extraordinary circumstances would be 120 days from the original disclosure obligation. Beyond the final 60-day delay, if the Attorney General indicates that further delay is necessary, the Commission may grant such additional relief through exemptive order.

[21] Final Rule at 36.

[22] Final Rule at 40.

[23] Final Rule at 41.

[24] Final Rule at 41.

[25] Final Rule at 41.

[26] Final Rule at 42.

[27] Final Rule at 41-42.

[28] Final Rule at 41-45.

[29] Final Rule at 43.

[30] Final Rule at 43.

[31] Final Rule at 61. See 17 CFR 229.106(b)(1).

[32] Final Rule at 61.

[33] Final Rule at 62.

[34] Final Rule at 62.

[35] Final Rule at 62-63.

[36] Final Rule at 68.

[37] Final Rule at 69-70.

[38] Final Rule at 85, 87.

[39] Final Rule at 88.

[40] Final Rule at 95.

[41] Final Rule at 96.