JENNER & BLOCK

SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure by Public Companies

Publications

August 3, 2023
By: Charles D. Riely, Shoba Pillay, Brian R. Boch, Alexander J. May, Hannah Schwab

On July 25, 2023, the US Securities and Exchange Commission (the SEC), by a 3-2 vote, adopted final rules regarding cybersecurity risk management, strategy, governance and incident reporting by public companies (the Final Rules).[1] The Final Rules (1) are intended to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and material cybersecurity incidents by registrants that are subject to the reporting requirements of the Securities Exchange Act of 1934 (the Exchange Act), (2) create new current disclosure requirements requiring registrants to disclose material cybersecurity incidents that they experience and (3) require registrants to disclose, on an annual basis, material information regarding their cybersecurity risk management, strategy and governance. The Final Rules apply to all public companies that are subject to the reporting requirements of the Exchange Act, except for asset-backed issuers.

The Final Rules will become effective 30 days after publication of the Adopting Release in the Federal Register. Information about key compliance dates is provided in the subsection below entitled "Effective Date and Compliance Dates." This alert (1) summarizes the key aspects of the Final Rules in a chart, (2) analyzes each component of the Final Rules in greater detail and (3) outlines some key takeaways that a public company could consider as it prepares for the effectiveness of these new rules.

Rule Amendments at a Glance	
New Form 8-K Item 1.05 – *Material Cybersecurity Incidents*	• If a registrant experiences a cybersecurity incident that it determines to be material, it will be required to describe in a Form 8-K: • The material aspects of the nature, scope and timing of the incident; and

	• The material impact or reasonably likely material impact on the company, including its financial condition and results of operations. • The Form 8-K will need to be filed within ***four*** business days after the registrant determines that it has experienced a material cybersecurity incident, subject to two limited exceptions: (1) where the United States Attorney General determines that disclosure poses a substantial risk to national security or public safety or (2) for compliance with certain Federal Communications Commission (FCC) notification rules that allow for the registrant to delay disclosure. • If relevant information required to be disclosed is not yet determined or otherwise available at the time of the required filing, the registrant must include a statement to that effect in the Form 8-K. • The registrant must then amend the prior Form 8-K to disclose such information within four business days after the information is determined or otherwise becomes available, without unreasonable delay. • Untimely filing of an Item 1.05 event will not result in the loss of Form S-3 eligibility.
New Regulation S-K Item 106(b) – *Risk Management and Strategy*	• A registrant will be required to describe its processes, if any, in its Form 10-K for assessing, identifying and managing material risks from cybersecurity threats, as well as whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially

	affected or are reasonably likely to materially affect the registrant.

New Regulation S-K Item 106(c) – *Governance*	• A registrant will be required to describe in its Form 10-K:
	  • The board's oversight of risks from cybersecurity threats.
	  • If applicable, the registrant will also need to identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which they are informed about such risks.
	  • Management's role in assessing and managing material risks from cybersecurity threats.

New Item 16K of Form 20-F– *Cybersecurity* and Amended General Instruction B of Form 6-K	• A foreign private issuer (FPI) will be required to provide the same type of disclosure as domestic issuers detailed above. • Material cybersecurity incidents may trigger an obligation for the FPI to file a current report on Form 6-K. • A FPI will need to furnish on Form 6-K information on material cybersecurity incidents that it discloses or otherwise publicizes in a foreign jurisdiction, to any stock exchange, or to security holders.

Summary of Key Changes

1. The New Requirement to Describe Material Cybersecurity Incidents Within Four Business Days on Form 8-K

New Item 1.05 of Form 8-K will require a registrant to disclose information related to cybersecurity incidents, as defined in new Item 106(a) of Regulation S-K,[2] within four business days after the registrant determines that the cybersecurity incident is material. The required disclosure will include a description of:

- The material aspects of the nature, scope and timing of the incident; and
- The material impact, or reasonably likely material impact, on the company, including its financial condition and results of operations.[3]

The triggering event for an Item 1.05 Form 8-K is the company's determination that a cybersecurity incident is material, not the company's discovery of the incident.[4] Significantly, Item 1.05 focuses the requisite disclosure primarily on the impact of the material incident, rather than the underlying details of the incident.[5] The SEC highlighted that a registrant's materiality analysis should include both qualitative and quantitative factors.[6] Item 1.05 disclosure can also be triggered by cybersecurity incidents on third-party systems that a registrants uses (such as cloud-based or software-based systems), and the SEC declined to offer a safe harbor (as proposed by comments received) for disclosures made about such third-party systems. Consequently, registrants will need to be mindful that other companies may be disclosing (or not disclosing) cybersecurity incidents that are caused by widely-used third-party systems based on each company's own version of materiality. [7] The SEC, in declining to adopt a safe harbor for third-party systems, observed that a registrant will need to disclose the information that is available to the registrant, and a registrant will not be required to conduct inquiries outside of any regular channels of communication with third-party service providers pursuant to such third-party contracts in determining the facts related to a third-party breach.[8]

A company must file its Form 8-K within ***four*** business days of making such a determination that a cybersecurity incident is material.[9] However, Instruction 1 to Item 1.05 of Form 8-K makes clear that a company must make its materiality determination about a cybersecurity incident without unreasonable delay, and the new Item 1.05 of Form 8-K does not provide discretion to delay reporting while an internal or external investigation is ongoing.[10]

For example, the SEC noted in the Adopting Release that for incidents impacting key systems and information or involving unauthorized access to or exfiltration of key information (e.g., its "crown jewels" information) or large quantities of particularly important data, the company may be able to determine materiality even without complete information about the incident.[11] Additional examples indicated by the SEC to involve unreasonable delay include:

- If the materiality determination is made by a board committee, intentionally deferring the committee's meeting on the determination past the normal time it takes to convene committee

members; and

- Revising existing incident response policies and procedures in order to support a delayed materiality determination, such as by:
  - extending the incident severity assessment deadlines;
  - changing the criteria that would require reporting the incident to management or committees responsible for public disclosures; or
  - introducing other steps to delay the determination or disclosure.[12]

Item 106(a) of Regulation S-K defines such terms as "cybersecurity incident" that are used in Item 1.05.[13] In the Final Rules, the SEC clarified that "a series of related unauthorized occurrences" falls within the definition of "cybersecurity incident."[14] As such, when a company finds that it has been materially affected by what may appear as a series of related cyber intrusions, Item 1.05 may be triggered even if each individual intrusion is immaterial on its own.

However, the Final Rules do include two exceptions that allow for delays in the Item 1.05 Form 8-K filing deadline under two limited circumstances.

First, new Item 1.05(c) of Form 8-K provides a limited exception to delay disclosure where, if the United States Attorney General determines that disclosure required by Item 1.05(a) of Form 8-K poses a substantial risk to national security or public safety and notifies the SEC of such determination in writing, the registrant may delay providing the disclosure required by Item 1.05 of Form 8-K for a time period specified by the Attorney General, up to 30 days following the date when the disclosure was otherwise required to be provided.[15] Under Item 1.05(c) of Form 8-K, disclosure may be delayed for an additional period of up to 30 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing.[16] In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security and notifies the SEC of such determination in writing.[17] Item 1.05(c) further provides that, beyond the final 60-day delay under Item 1.05(c), if the Attorney General indicates that further delay is necessary, the SEC will consider additional requests for delay and may grant such relief though SEC exemptive order.[18]

In the Adopting Release, the SEC noted that the SEC has consulted with the US Department of Justice (DOJ) to establish an interagency communication process to allow for the Attorney General's determination to be communicated to the SEC in a timely manner, and that the DOJ will notify the affected registrant that communication to the SEC has been made, so that the registrant may delay filing its Form 8-K.[19] It is not yet clear how this exception will operate as a practical matter.

Second, the new Item 1.05(d) of Form 8-K provides a limited exception to delay disclosure for compliance with certain FCC notification rules.[20] This exception provides that registrants may delay the filing of the Item 1.05 Form 8-K for up to the ***seven***-business-day period following notification to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) specified in the FCC rule for breaches of customary proprietary network information (CPNI), with written notification to the SEC of such delay.[21] The SEC added this exception to accommodate registrants who are subject to both FCC notification rules and the Final Rules and could face conflicting disclosure timelines when such registrant experiences a CPNI breach.[22] However, the exception is limited to the initial seven-business-day period after notification to the USSS and FBI and may not be further delayed, except as described above in connection with a substantial risk to national security or public safety.[23]

To help solve for the uncertainties inherent in cybersecurity disclosures, Instruction 2 to Item 1.05 provides that where information called for in Item 1.05 has not been determined or is unavailable, the company must include a statement to that effect in its filing.[24] Once the company determines that information, or it becomes available, the company would then need to file an amendment to its Form 8-K providing the information within four business days of such determination or availability.[25]

In addition, Instruction 4 to Item 1.05 also codifies the SEC's assurance from its March 2022 proposal release[26] that a company's disclosures do not need to include specific or technical information about its planned incident response or its cybersecurity systems in such detail as would impede its response or remediation of the incident.[27]

Importantly, the Final Rules also added Item 1.05 to the list of Form 8-K items in General Instruction I.A.3.(b) of Form S-3, so that any untimely filing of an Item 1.05 Form 8-K will not trigger the loss of Form S-3 eligibility, so long as the company is current in its Form 8-K reporting at the time the Form S-3 is filed.[28] Further, the Final Rules also amended Exchange Act Rules 13a-11(c) and 15d-11(c) to include Item 1.05 in the list of Form 8-K items eligible for a limited safe harbor from liability under Exchange Act Section 10(b) and Exchange Act Rule 10b5-1.[29]

Since FPIs do not have Form 8-K filing obligations, the Final Rules also amended General Instruction B of Form 6-K to reference material cybersecurity incidents among the items that may trigger an obligation for a FPI to file a current report on Form 6-K.

2. <u>The New Disclosure Requirements Related to Risk Management, Strategy and Governance</u>

The SEC also adopted new Item 106 of Regulation S-K, which will require disclosure related to a company's cybersecurity risk management, strategy and governance in its annual report on Form 10-K.[30] The Final Rules also amended Form 20-F to add new Item 16K, which will require FPIs to

provide the same type of disclosure as domestic issuers will be required to provide under new Item 106 of Regulation S-K.[31]

New Item 106(b)(1) of Regulation S-K will require a registrant to describe its processes, if any, for assessing, identifying and managing material risks from cybersecurity threats.[32] Such disclosure will need to be detailed enough for a reasonable investor to understand those processes and address the following non-exhaustive list of disclosure items, as applicable:

- Whether and how the described processes have been integrated into the company's overall risk management system or processes;
- Whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
- Whether the company has processes to oversee and identify material risks from the cybersecurity threats associated with its use of any third-party service provider.[33]

New Item 106(b)(2) of Regulation S-K will also require a registrant to disclose whether and how any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected, or are reasonably likely to materially affect, the company, including its business strategy, results of operations or financial condition.[34]

New Item 106(c) of Regulation S-K will require a registrant to provide disclosures regarding its board of directors' and management's role in overseeing cybersecurity risks.[35] Specifically, a registrant will need to:

- Describe the board's oversight of risks from cybersecurity threats and, if applicable, identify any board committee or subcommittee responsible for cybersecurity risk oversight and the processes by which the board or such committee is informed about cybersecurity risks[36] ; and
- Describe management's role in assessing and managing material risks from cybersecurity threats. The company's description should address, as applicable, the following non-exhaustive list of disclosure items:
    - Whether and which management positions or committees are responsible for assessing and managing such risks, and 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.[37]

Disclosures required under Item 106 of Regulation S-K will need to be contained in Part I of a registrant's Form 10-K under a new Item 1C. Unlike similar governance and risk disclosures under Item 407 of Regulation S-K or contained in Part III of Form 10-K, a registrant will not be able to disclose this new information about cybersecurity risk oversight in a proxy statement for incorporation by reference into the Form 10-K.

3. Inline XBRL Formatting

The Final Rules will require that all information specified in Item 1.05 of Form 8-K and Item 106 of Regulation S-K be presented in Inline XBRL in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual. However, the structured data requirements will be subject to a one-year transition period.[38]

4. Effective Date and Compliance Dates

The Final Rules will become effective 30 days after publication of the Adopting Release in the Federal Register. Compliance will be required as follows:

- All registrants will need to provide disclosures required under Item 106 of Regulation S-K, or Item 16K, beginning with their first annual reports for fiscal years ending on or after December 15, 2023.
    - Thus, for a registrant with a fiscal year ending on December 31, 2023, Item 106 information will be required to be disclosed in its Form 10-K that will be filed in early 2024.
- All registrants, other than smaller reporting companies (SRCs), will need to comply with the incident disclosure requirements in Item 1.05 of Form 8-K and Form 6-K beginning 90 days after the date the Adopting Release is published in the Federal Register, or December 18, 2023, whichever is later.
    - SRCs will need to comply with the incident disclosure requirements beginning 270 days after the date the Adopting Release is published in the Federal Register, or June 15, 2024, whichever is later.

Key Impacts and Considerations

The following are some takeaways that a company could consider as it prepares for the Final Rules to become effective:

1. Be Prepared to Make Nimble Materiality Determinations as Part of the Company's Cybersecurity Incident Response Plan and Under the Company's Disclosure Controls and Procedures

The Final Rules will require a registrant to make prompt materiality determinations, as well as ongoing materiality assessments, while simultaneously addressing the underlying cybersecurity incident.[39] The SEC has made clear that a registrant will not be able to delay its disclosure decisions based on the need to investigate,[40] and in fact, a registrant that takes steps to evaluate materiality outside its normal course might raise concerns of "unreasonable delay."[41] Accordingly, a public company may find it prudent to consider its policies and procedures for responding to a cybersecurity incident, along with assessing the materiality of, and potential need to disclose, an incident, well before the company is immersed in crisis control.

Significantly, the SEC in adopting the Final Rules declined to adopt a quantifiable trigger for materiality, indicating that "some cybersecurity incidents may be material yet not cross a particular financial threshold."[42] Rather, the standard for materiality will be consistent with existing cases addressing materiality in securities laws,[43] as well as Securities Act of 1933 (the Securities Act) Rule 405[44] and Exchange Act Rule 12b-2.[45] Furthermore, the Adopting Release highlights that while the Final Rules will require that a registrant describe in its Form 8-K "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," the Final Rules' inclusion of "financial condition and results of operations" is not exclusive, and companies should consider both qualitative and quantitative factors in assessing the material impact of an incident.[46] Additional examples of what may constitute a material impact, or a reasonably likely material impact, include:

- Harm to the company's reputation, customer or vendor relationships, or competitiveness; and
- The possibility of litigation or regulatory investigations or actions, including actions by state and Federal authorities and non-US authorities.[47]

In his statement, Commissioner Jaime Lizárraga added that material impact could include intellectual property loss, business interruption, and increased costs of capital.[48] Ultimately, neither the Final Rules nor the Adopting Release provide a limiting principle for when the impact of a cybersecurity incident could be considered immaterial for purposes of disclosure.

In their respective statements, Commissioner Hester M. Peirce and Commissioner Mark T. Uyeda each commented on this aspect of the Final Rules. Commissioner Peirce noted that the SEC, in adopting the Final Rules, "reject[ed] financial materiality as the touchstone for its disclosures, and fail[ed] to offer in its place a meaningful intelligible limit to its disclosure authority."[49] Commissioner Uyeda similarly observed that the Final Rules have taken the unprecedented step of "requiring real-time, forward-looking disclosure" in Form 8-K filings regarding estimates such as remediation costs, as well as constant assessments for amendment to disclose material impacts that were not determined at the time of the initial filing.[50]

Recent cybersecurity cases underscore the importance of well-functioning disclosure controls and procedures to ensure a company is making appropriate disclosures even as its investigation is ongoing.[51] In those cases, the SEC penalized companies that disclosed—but downplayed—a cybersecurity incident based on incomplete information, noting that these companies should have had better escalation policies to ensure that more substantive information about a cybersecurity incident would be passed up the chain to the people making disclosure decisions. These cases foreshadow that the SEC will likely continue to scrutinize every cybersecurity disclosure—from initial, to interim, to final statements—for timeliness and accuracy by comparing the disclosure to the information that was contemporaneously available to the company.

In light of the foregoing, a public company may find it prudent to reexamine its incident response policies and procedures in two respects: (1) to ensure that its incident response policies and procedures incorporate the relevant qualitative and quantitative factors that will inform the materiality determination; and (2) to ensure that the incident escalation process is well-functioning and will provide relevant, real-time information regarding an incident to the right disclosure personnel. These steps could help ensure that a company would have a well-established blueprint for handling a cybersecurity incident and that its disclosure decisions would reflect careful, well-substantiated, and documented judgment.

2. Continuously Review Current Risk Management and Governance Practices Against Item 106 Disclosure Requirements to Ensure Best Practices and Accurate Disclosures

New Item 106 of Regulation S-K contains a non-exclusive list of disclosure requirements for registrants to address, as applicable, when describing their overall risk management program for cybersecurity incidents and how cybersecurity incidents are managed at the board level. To help provide accurate and meaningful disclosure, a registrant could consider such activities as:

- Modifying D&O questionnaires to inquire about board and management expertise about cybersecurity risk management;
- Ensuring that there are clear reporting mechanisms within management, the board and its committees, and that such mechanisms can be documented for disclosure in the Form 10-K;
- Modifying board committee charters and/or corporate governance guidelines to specifically provide for cybersecurity responsibilities;
- Documenting cybersecurity activities by the board and its committees in the minutes of such bodies; and
- Cataloging and monitoring the work of third-party vendors that support the registrant's cybersecurity function.

3. Review the Company's Cybersecurity Risk Factors in Light of Risk Management and Governance Disclosures to Ensure Consistent Messaging

A public company may find it prudent to review, and consider updating, its cybersecurity risk factors in light of the required risk management and governance disclosures to ensure that the risk factors contain consistent messaging with the disclosure requirements and to identify updates that may be required in the issuer's next Form 10-K or 20-F, as applicable.

As previously discussed above, the SEC has already brought numerous cases against public companies that identified data incidents as a hypothetical risk factor but failed to update this disclosure when information about a known cybersecurity incident became available.[52] These cases emphasize the need for heightened scrutiny around cybersecurity risk factor disclosures. In particular, it may be prudent for a registrant to consider the process by which it will update its existing risk factors should Item 1.05 disclosure be required in response to a cyber incident.

4. Additional Internal Education; Additional Anticipated Costs of Compliance

Relatedly, a registrant may find it prudent to consider educating its board of directors, officers and key employees about the requirements of the Final Rules and the company's applicable policies and procedures, including its incident response preparedness and training, to ensure it has a well-functioning escalation process for incidents and proper integration of these processes with the company's disclosure controls and procedures to ensure timely and appropriate disclosures.

A company should also expect to encounter increased costs associated with complying with the Final Rules.[53]

The Final Rules present significant challenges in compliance. Jenner & Block is pleased to counsel its clients regarding the Final Rules, and can assist with preparation of best practices, as well as provide crisis management and compliance counseling in the event of an actual cybersecurity incident.

Charles D. Riely, Shoba Pillay, Brian R. Boch, Alexander J. May and Jennifer Lee are partners and Hannah E. Schwab is an associate with Jenner & Block LLP.

Footnotes

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11216; 34-97989 (July 26, 2023), available at www.sec.gov/rules/final/2023/33-11216.pdf [hereinafter, the Adopting Release].

[2] *See* Item 106(a) of Regulation S-K (A "cybersecurity incident" is defined 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.").

[3] *See* Item 1.05 to Form 8-K.

[4] *See* Adopting Release, at 32.

[5] *Id.* at 29.

[6] *Id.* at 37 ("For example, an incident that results in significant reputational harm to a registrant may not be readily quantifiable and therefore may not cross a particular quantitative threshold, but it should nonetheless be reported if the reputational harm is material. Similarly, whereas a cybersecurity incident that results in the theft of information may not be deemed material based on quantitative financial measures alone, it may in fact be material given the impact to the registrant that results from the scope or nature of harm to individuals, customers, or others, and therefore may need to be disclosed.").

[7] *Id.* at 31 ("Depending on the circumstances of an incident that occurs on a third-party system, disclosure may be required by both the service provider and the customer, or by one but not the other, or by neither.").

[8] *Id.*

[9] *Id.* at 37.

[10] *See* Instruction 1 to Item 1.05 to Form 8-K; Adopting Release, at 15.

[11] *See* Adopting Release, at 37-38.

[12] *Id.* at 38.

[13] *See* Item 106(a) of Regulation S-K.

[14] *See* Adopting Release, at 52-53.

[15] *See* Item 1.05(c) to Form 8-K; Adopting Release, at 34.

[16] *Id.*

[17] *Id.* at 35.

[18] *Id.*

[19] *Id.*

[20] *See* Item 1.05(c) of Form 8-K.

[21] *See* 47 CFR 64.2011; the FCC's rule for notification in the event of a breach of CPNI, requires a covered entity to notify the USSS and FBI no later than seven business days after reasonable determination of a CPNI breach, and further directs the covered entity to refrain from notifying customers or disclosing the breach publicly until seven business days have passed following such notification. CPNI is defined in 47 CFR 222(h)(1) as: "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications

carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information."

[22] *See* Adopting Release, at 42. Such notification to the SEC will be required to be made under the banner of CORRESP through EDGAR no later than the date when the disclosure required by Item 1.05 was otherwise required to be provided.

[23] *Id.* (noting "[t]he exception we are creating does not apply to 47 CFR 64.2011(b)(3), which provides that the USSS or FBI may direct the entity to further delay notification to customers or public disclosure beyond seven business days if such disclosure 'would impede or compromise an ongoing or potential criminal investigation or national security.' If the USSS or FBI believes that disclosure would result in a substantial risk to national security or public safety, it may, as explained above, work with the Department of Justice to seek a delay of disclosure.").

[24] *See* Instruction 2 to Item 1.05 to Form 8-K.

[25] *Id.*

[26] *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038, 16595 (Mar. 9, 2022), available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

[27] *See* Instruction 4 to Item 1.05 to Form 8-K.

[28] *See* Adopting Release, at 39.

[29] *Id.*

[30] *Id.* at 53.

[31] *Id.* at 176.

[32] *See* Item 106(b)(1) of Regulation S-K.

[33] *See* Adopting Release, at 62-63.

[34] *See* Item 106(b)(2) of Regulation S-K.

[35] *See* Adopting Release, at 68-71.

[36] *See* Item 106(c)(1) of Regulation S-K.

[37] *See* Item 106(c)(2) of Regulation S-K.

[38] *See* Adopting Release, at 88-89. For Item 106 of Regulation S-K, all registrants will need to begin tagging responsive disclosure in Inline XBRL beginning with annual reports for fiscal years ending on or after December 15, 2024; and for Item 1.05 of Form 8-K and Form 6-K all registrants will need to begin tagging responsive disclosure in Inline XBRL beginning on December 18, 2024, or 465 days after the date of publication of the Final Rules in the Federal Register, whichever is later.

[39] *Id.* at 36.

[40] *Id.* at 29.

[41] *Id.*at 38.

[42] *Id.* at 36.

[43] *Id.* at 80 (citing *TSC Industries, Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1976) (holding that 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); *Basic, Inc. v. Levinson*, 485 U.S. 224, 232 (1988); *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27 (2011)).

[44] *See* 17 CFR 230.405.

[45] *See* 17 CFR 240.12b-2.

[46] *See* Adopting Release, at 29-30.

[47] *Id.*

[48] *See* Improving the Quality of Cybersecurity Risk Management Disclosures of Comm'r Jaime Lizárraga (Jul. 26, 2023), available at https://www.sec.gov/news/statement/lizarraga-statement-cybersecurity-072623.

[49] *See* Harming Investors and Helping Hackers: Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure of Comm'r Hester M. Peirce (Jul. 26, 2023), available at https://www.sec.gov/news/statement/peirce-statement-cybersecurity-072623 [hereinafter, the Peirce Statement].

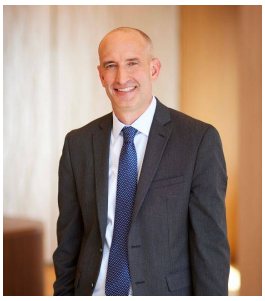
[50] *See* Statement on the Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure of Comm'r Mark T. Uyeda (Jul. 26, 2023), available at https://www.sec.gov/news/statement/uyeda-statement-cybersecurity-072623.

[51] S*ee, e.g.,* Press Release, US Sec. & Exch. Comm'n, SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors (Mar. 9, 2023), available at https://www.sec.gov/news/press-release/2023-48; Press Release, US Sec. & Exch. Comm'n, SEC Charges Pearson plc for Misleading Investors About Cyber Breach (Aug. 21, 2021), available at https://www.sec.gov/news/press-release/2021-154.

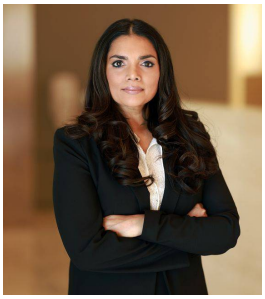
[52] *Id.*

[53] *See* Peirce Statement (stating that the Final Rules "may serve to drive companies to spend resources on compliance with our rules and conformity with other companies' disclosed practices, instead of on combatting cyber threats as they see fit," and that "[c]osts likely will be disproportionately high (and the benefits may be disproportionately low) for investors in small public companies, for which the Commission has provided only one accommodation—an extra 180 days to comply with the 8-K requirement").

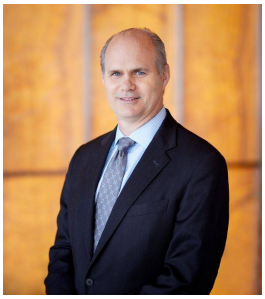
Related Attorneys



Charles D. Riely
Partner
criely@jenner.com
+1 212 891 1686

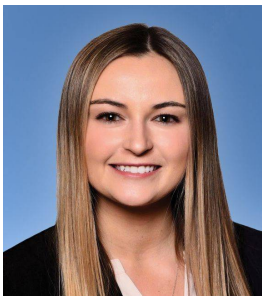


Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605



Brian R. Boch
Partner
bboch@jenner.com
+1 312 923 2880

Alexander J. May
Partner
amay@jenner.com
+1 312 840 8659



Hannah Schwab
Associate
hschwab@jenner.com
+1 312 840 7331

Related Capabilities

Corporate

Data Privacy and Cybersecurity

Investor and Securities Litigation

Securities and Capital Markets

Stay Informed →