MAYER | BROWN

July 28, 2023

Legal Update

SEC Adopts Final Rules on Public Company Cybersecurity Disclosures of Incidents and Processes

Background and Summary Table

On July 26, 2023, the U.S. Securities and Exchange Commission (the "SEC") issued a release (the "Adopting Release"), adopting final rules (the "Final Rules") aimed at standardizing and enhancing disclosure relating to cybersecurity incidents and risk management processes.[1] The SEC had proposed rules (the "Proposed Rules") on March 9, 2022.[2] The Final Rules reflect the considerable comments received on the Proposed Rules, resulting in far narrower and streamlined requirements, though still imposing significant new requirements on registrants.

The SEC has focused on cybersecurity issues for some time, having provided staff guidance in 2011 and a report detailing its investigation of several public companies that were victims of cybersecurity-related incidents. In 2018, the SEC issued interpretive guidance requiring public companies to disclose material cybersecurity risks and incidents. Registrants already provide significant disclosures in their periodic reports and offering materials regarding cyber risks, incidents, and related investigations or litigation to the extent material. In fact, the Adopting Release, in its economic analysis, noted that disclosures of efforts to mitigate cybersecurity risk were found in 99 percent of proxy statements or Forms 10-K from 2020 to 2022.[3]

With the Final Rules, public companies will be required to report (1) material cybersecurity **incidents** and (2) cybersecurity risk management **processes** in a more standardized manner, subject to specific timelines, in order to provide greater comparability of disclosures. The information required to be disclosed under the Final Rules, as well as the timing and the means of disclosure, are summarized in the following table, followed by detailed discussion and concluding with practical considerations for company general counsel and other officers and directors.

Final Rule	What to disclose	When to disclose
Incident Disclosures: Item 1.05 of Form 8-K.	Disclose any cybersecurity incidents determined to be material and describe the material aspects of • the nature, scope and timing of the incident; and • the impact or reasonably likely impact of the incident on the registrant, including on the registrant's financial condition and results of operations. The registrant need *not* disclose specific or technical information about its planned response to the incident or its cybersecurity systems, or potential system vulnerabilities, in such detail as would impede the registrant's response or remediation of the incident.	• Disclose within four business days after the registrant determines it has experienced a *material* cybersecurity incident. • A registrant must determine whether a cybersecurity incident is material "without unreasonable delay." • A registrant may delay filing an Item 1.05 on Form 8-K if the United States Attorney General determines that immediate disclosure would pose substantial risk to national security or public safety.
Incident Disclosures: Amendment to Item 1.05 of Form 8-K.	Include a statement in its Item 1.05 on Form 8-K to identify information that was either • not determined when the initial Form 8-K was filed; or • unavailable when the initial Form 8-K was filed.	The amendment to Item 1.05 on Form 8-K must be filed within four business days after either: • the registrant, without unreasonable delay, determines such information exists; or • the information to be disclosed in the amendment becomes available.
Process Disclosures: Item 106(b) of Regulation S-K.	Describe • processes, if any, to identify, assess and manage cybersecurity risks; and • whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect business strategy, results of operations, or financial condition.	Disclose in registrant's annual report (*i.e.*, Form 10-K).
Process Disclosures: Item 106(c)(1) of Regulation S-K.	Describe the Board of Directors' oversight of cybersecurity risk. Registrants need *not* disclose information about the frequency of board discussions of cybersecurity or information about any director expertise in the field.	Disclose in registrant's annual report (*i.e.*, Form 10-K).
Process Disclosures: Item 106(c)(2) of Regulation S-K.	Describe management's role in assessing and managing material risks from cybersecurity threats.	Disclose in registrant's annual report (*i.e.*, Form 10-K).
Final Rules affecting Foreign Private Issuers		
Amendment to General Instruction B of Form 6-K.	Foreign private issuers ("FPIs") must furnish on Form 6-K information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders.	Disclose timely, in a manner consistent with the general purpose and use of Form 6-K.
Item 16J on Form 20-F.	FPIs must describe • Board's oversight of risks from cybersecurity threats; • Management's role in assessing and managing material risks from cybersecurity threats.	Disclose in FPI's annual report only (*i.e.*, Form 20-F).

Final Rules

The Final Rules encompass **incident disclosure** and **process disclosure** and differ in important ways from the Proposed Rules, as detailed below.

Incident Disclosure

The Final Rules establish a new Item 1.05 of Form 8-K, requiring registrants to disclose information about a cybersecurity incident within four business days after the registrant determines that it has experienced a "material" cybersecurity incident. The Final Rules take into account many concerns raised by commenters. The SEC revised the Proposed Rules in scope and provide a delay for disclosures that pose a substantial risk to national security or public safety.

Scope of incident disclosure. The information required to be disclosed is narrowed. The Proposed Rules would have required a registrant to disclose certain detailed information about a material cybersecurity incident, if known at the time of filing.[4] The SEC noted commenters' concerns that the disclosure of certain details as proposed would exacerbate cybersecurity threats and lessen threat information-sharing within industries. The SEC streamlined Item 1.05 to focus primarily on disclosing the *impact* of the material cybersecurity incident, rather than details regarding the incident itself. The SEC opines that this would more precisely focus the disclosure on what the company views as the material impact of the incident, which may vary from incident to incident, describing "the material aspects of the nature, scope and timing of the incident, and the material impact or reasonably likely impact on the registrant, including its financial condition and results of operations."

The SEC also clarified that the reference to "financial condition and results of operations" in the Final Rule is not the exclusive test of materiality. The Adopting Release affirms the view expressed in the Proposing Release that the materiality standard should be consistent with that expressed in classic cases such as *TSC Industries, Inc.*, *Basic, Inc.* and *Matrixx Initiatives*. 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."[5] Therefore, materiality may also be indicated by qualitative impacts, such as the possibility of litigation or regulatory investigations, reputational harm, impact on customer or vendor relationships, or a registrant's competitiveness. In a further change from the Proposed Rules, there is no requirement to disclose the remediation status of the cybersecurity incident, whether the incident is ongoing, and whether data were compromised.

The SEC added Instruction 4 to Item 1.05 to clarify that a registrant need not disclose "specific or technical information about its planned response to the incident . . . in such detail as would impede the registrant's response or remediation of the incident."

Commenters questioned whether Item 1.05 would require disclosure of a cybersecurity incident occurring on a third-party system used by the registrant, instead of an incident directly affecting the registrant's internal systems. The SEC stated its position that "whether an incident is material is not contingent on where the relevant electronic systems reside or who owns them." Disclosure of the incident may be required by both, either or neither the service provider and the customer, depending on the circumstances of the cybersecurity incident that occurs on a third-party system.

Timing of incident disclosure. Under the Final Rules, the obligation to file an Item 1.05 of Form 8-K is triggered by the registrant's determination that a cybersecurity incident is material. As discussed above,

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."

The registrant must file the Form 8-K within four business days after the materiality determination. As proposed, Instruction to Item 1.05 would have required that determinations of materiality be made "as soon as reasonably practicable after discovery of the incident." In the Final Rules, the SEC revised this Instruction to state that the materiality determination must be made "without unreasonable delay."

The SEC indicated that the registrant's determination of materiality would generally provide the registrant with the information required to fulfill its disclosure obligations under this Item 1.05, and therefore opines that the four business day timeline is workable. Additionally, the SEC adopted its proposed amendment to General Instruction I.A.3.(b) of Form S-3 such that a late filing on Form 8-K regarding the new item 1.05 would not cause the registrant to lose eligibility for Form S-3.[6] Furthermore, while some commenters had suggested that Item 1.05 could be furnished rather than filed, the SEC opined that treating Item 1.05 disclosures as filed would promote the accuracy and reliability of such disclosures.

In another change from the Proposed Rules, the SEC adopted a delay provision in cases where disclosure of a cybersecurity incident would pose a substantial risk to national security or public safety. Pursuant to Item 1.05(c) of Form 8-K, a registrant may delay making an Item 1.05 Form 8-K filing, if the Attorney General determines that the disclosure poses a substantial risk to national security or public safety and notifies the SEC of such determination in writing.

The disclosure may be delayed by a time period specified by the Attorney General for up to 30 days, may be extended for an additional period of 30 days and, in extraordinary circumstances, the Attorney General may further delay disclosure for a final additional period of up to 60 days. The SEC reports that it has consulted with the Department of Justice to establish an interagency communication process to facilitate such determinations. The SEC stated its position that the Final Rules balance security concerns against investors' informational needs.

The delay provision as adopted is not equivalent to the "law enforcement delays" provided in many state data breach notification laws. Such provisions allow companies, at the request of law enforcement, to delay providing required notifications to regulators or individuals to facilitate ongoing investigations. Although the Final Rules do not prevent any law enforcement agency from requesting the Attorney General to determine that disclosure should be delayed, the SEC stated its belief that designating a single agency as the SEC's point of contact was critical to ensuring that the Final Rules are administrable.

The SEC considered potential conflicts with other Federal laws and regulations and identified a conflicting disclosure obligation with the FCC's notification rule for breaches of customary proprietary network information ("CPNI"). The FCC's rule for notification in the event of breaches of CPNI requires covered entities to notify the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") no later than seven business days after reasonable determination of a CPNI breach, and further directs the entities to refrain from notifying customers or disclosing the breach publicly until seven business days have passed following the notification to the USSS and FBI. To accommodate registrants subject to this rule and may face conflicting disclosure timelines, the SEC added paragraph (d) to Item 1.05 providing that such registrants may delay making a Form 8-K disclosure up to the *seven* business day period following notification to the USSS and FBI specified in the FCC rule, with written notification to the SEC.

Updating incident disclosure. Under the Proposed Rules, Item 106(d) of Regulation S-K would have required disclosure of "any material changes, additions or updates to information required to be disclosed pursuant to Item 1.05 of Form 8-K" in the registrant's quarterly report filed on Form 10-Q or annual report filed on Form 10-K. Proposed Item 106(d)(1) also would have required registrants to disclose information that was not available at the time of the initial Form 8-K filing would be disclosed in the registrant's subsequent periodic filing.

Instead of adopting Item 106(d)(1) as proposed, the SEC added Instruction 2 to Item 1.05 of Form 8-K, directing a registrant (i) to identify any information that is not determined or unavailable at the time of the required filing and (ii) file an amendment to its initial Form 8-K, containing such information. An amendment must be filed within four business days after the registrant, without unreasonable delay, determines the missing information, or within four business days after such information becomes available. The SEC considered that this change would, among other things, allow investors to more quickly identify updates regarding previously disclosed cybersecurity incidents. The SEC also noted that registrants have an obligation to correct prior disclosure or to update disclosure that becomes materially inaccurate.

The SEC also did not adopt proposed Item 106(d)(2), which would have required disclosure when a series of cybersecurity incidents that are immaterial individually become material in the aggregate. The SEC received comments that the aggregation requirement was vague or difficult to apply. However, a similar aggregation concept was adopted in the Final Rules under the definition of "cybersecurity incident," revised in the Final Rules to include "a series of related unauthorized occurrences." This is intended to capture a series of smaller but continuous cyberattacks that become quantitatively or qualitatively material collectively or related attacks from multiple actors exploiting the same vulnerability.

Process Disclosure

The Final Rules require disclosures regarding (i) the registrant's processes, if any, for identifying and managing cybersecurity risks, (ii) the board of directors' role in oversight of cybersecurity risks, and (iii) management's role in managing cybersecurity-related risks and implementing the company's cybersecurity policies and procedures.

Compared to the Proposed Rules, the Final Rules narrow the disclosures required under Item 106(b)(1) of Regulation S-K. While Item 106(b)(1) as proposed would have required detailed disclosure, the Final Rules only require 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." The SEC stated its belief that the revised formulation avoids detail beyond what is material to investors. Item 106(b)'s enumerated disclosure elements were pared down in response to concerns regarding the level of detail required by the Proposed Rules.

As adopted, Item 106(b) provides that registrants should consider disclosing:

- whether and how the described cybersecurity processes in Item 106(b) have been integrated into the registrant's overall risk management system or processes;
- whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
- whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.

The SEC streamlined Item 106(c)(1) of Regulation S-K to require less granular disclosure. The Final Rules under Item 106(c)(1) require that registrants describe:

- the board of directors' oversight of risks from cybersecurity threats, and, if applicable, identify any board committee or subcommittee responsible for the oversight of cybersecurity risk; and
- if applicable, the processes by which the board or the applicable committee is informed about cybersecurity risks.

Unlike the Proposed Rules, Item 106(c)(1) under the Final Rules does not require the registrant to disclose the frequency of the board's discussions on cybersecurity risk, and whether and how the board considers cybersecurity risks as part of its business strategy, risk management and financial oversight.

The SEC also modified Item 106(c)(2) to add a materiality qualifier, requiring a registrant to describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. Under the Final Rules, Item 106(c)(2) provides that registrants should *address, as applicable,* the following non-exclusive topics as part of a description of management's role in assessing and managing the registrant's material risk from cybersecurity threats:

- whether and which management positions or committees are responsible for managing cybersecurity risk, and the relevant expertise of such persons;
- the processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection and remediation of cybersecurity incidents; and
- whether such persons or committees report on cybersecurity risk to the board of directors or a committee of the board of directors.

In the Final Rules, in response to many different substantial concerns raised in comment letters, the SEC did not adopt the proposed amendment to Item 407 of Regulation S-K which would have required a registrant to disclose whether any board member has cybersecurity expertise, and, if so, the nature of such expertise.

Foreign Private Issuers. The SEC adopted the Form 20-F and Form 6-K amendments as proposed, which would generally affect most FPIs. Form 20-F will be amended by adding Item 16J to require the same type of disclosure discussed above for domestic registrants in Item 106 of Regulation S-K. Similarly, cybersecurity incidents will now trigger a disclosure obligation on Form 6-K, if the FPI determines that it is material.

The SEC affirmed its stance in the Proposed Rules that there was no need to provide prescriptive cybersecurity disclosure requirements for Form 40-F filers, since the multijurisdictional disclosure system ("MJDS") generally permits eligible Canadian foreign private issuers to use Canadian disclosure standards and documents to satisfy the SEC's registration and disclosure requirements. The SEC noted that such filers are already subject to the Canadian Securities Administrators' 2017 guidance on the disclosure of cybersecurity risks and incidents, and thus would not need to require an MJDS issuer filing an annual report on Form 40-F to comply with the SEC's specific proposed cybersecurity-related disclosure requirements in the same manner as Form 10-K or Form 20-F filers.

Asset-Backed Issuers. The SEC exempted issuers of asset-backed securities that do not have any officers or directors from the Final Rules. The SEC expressed agreement with a commenter that the Final Rules would not result in meaningful disclosure by asset-backed issuers, which are typically special purpose vehicles that engage in the limited activity of receiving, purchasing, transferring or selling assets to an issuing entity and would

therefore not own or use information systems. The SEC indicated that it may consider specific cybersecurity disclosure rules applicable to asset-backed securities at a later date.

Smaller Reporting Companies. The SEC did not adopt an exemption for smaller reporting companies nor provide an additional compliance period for smaller reporting companies to comply with Item 106 of Regulation S-K. The SEC stated its belief that the streamlined requirements of the Final Rules as compared to the Proposed Rules would reduce some of the costs associated with the proposal for all registrants, including smaller reporting companies. The SEC also said that information regarding a registrant's existing cybersecurity strategy, risk management, and governance is factual, and therefore would be readily available to assess for purposes of preparing disclosure. The SEC stated that, given the significant cybersecurity risks faced by smaller reporting companies, and the outsized impacts that cybersecurity incidents may have, investors in smaller reporting companies require timely disclosure on material cybersecurity incidents and the material aspects of a smaller reporting company's cybersecurity risk management and governance. The SEC, however, provided smaller reporting companies with an additional 180 days from the non-smaller reporting company compliance date before compliance with Item 1.05 of Form 8-K is required.

Commission Authority. The SEC responded to certain comments, identifying and supporting its authority to regulate cybersecurity. Certain commenters argued that the SEC did not have authority to regulate cybersecurity disclosure. The SEC disagreed, however, citing that the authority granted by the Securities Act of 1933 and the Exchange Act are intentionally broad and empower the SEC to carry out its fundamental Congressional objectives. Of course, this may be subject to litigation challenge.

Structured Data Requirements. The SEC adopted the rule as proposed that all forms and disclosures described above be tagged in Inline XBRL in order to facilitate comparison and analysis of the data being disclosed.

Practical Considerations

Timetable. The timetable is tight. The Final Rules become effective 30 days following publication of the adopting release in the *Federal Register*. Reporting companies should note that the Form 10-K and Form 20-F disclosures will be due beginning with annual reports for fiscal years ending on or after December 15, 2023. For incident reporting, Form 8-K and Form 6-K disclosures will be due beginning the later of 90 days after the date of publication in the *Federal Register* or December 18, 2023. Smaller reporting companies will have an additional 180 days before they must begin providing the Form 8-K disclosure.

Responding to Cybersecurity Incidents. Companies should make appropriate updates to their cyber incident response plans and other preparedness activities in light of the requirements of the Rules and the associated challenges. Actions to consider include:

- ensuring that the incident response plan provides for appropriate stakeholders to be engaged and necessary facts to be gathered to allow a materiality determination to be made "without unreasonable delay" and to enable a timely subsequent disclosure;
- to the extent that the company believes that it might pursue a disclosure delay based on substantial risk to national security or public safety, developing an internal process through which appropriate stakeholders determine whether to seek such a delay in a particular incident and then seek such relief from the Justice Department;

- ensuring that incident response plans contemplate that disclosure may be required before an incident is contained, requiring the company to respond to a change in tactics by the threat actor or additional attacks by other malicious actors alerted to the company's vulnerability to attack;
- to the extent practicable, assessing in advance the factors that the company would need to take into account if it becomes necessary to determine if a specific cyber incident is material. In evaluating materiality, note that the rule cites the quantitative impact on financial condition and results of operations, while also noting that qualitative factors may contribute as well, giving as examples harm to reputation, relationships, and competitive position;
- evaluating how the required public disclosure of the incident may affect other aspects of the incident response process, such as triggers for convening of internal teams and executive escalation, notification to law enforcement or other government agencies, and engagement with customers, business partners, or other third parties, and making corresponding changes to the incident response plan; and
- practicing use of these new or revised processes through appropriate tabletop exercises and making further process changes based on lessons learned during the exercises.

Updating Processes. Companies should consider updating their disclosure controls and procedures to reflect both the new current reporting requirements for cyber incidents, including the potential need for amendments and the annual disclosure requirements. Companies may also want to consider if their internal controls over financial reporting need any adjustment in light of the SEC's new cybersecurity risk management, strategy governance and incident disclosure rules. In such exercises, it may be helpful to note how the SEC emphasizes a deliberate word choice, saying: "we substituted the term 'processes' for the proposed 'policies and procedures' to avoid requiring disclosure of the kinds of operational details that could be weaponized by threat actors, and because the term 'processes' more fully compasses registrants' cybersecurity practices than 'policies and procedures,' which suggest formal codification."

Balancing Investor Protection with Improvident Disclosure. The balance between investor protection and improvident disclosure is always delicate. In this case, companies must make materiality determinations "without unreasonable delay" and, without careful planning, may find that a quick public disclosure makes it difficult to accurately assess and effectively respond to a rapidly evolving cybersecurity incident. Companies may not have an adequate opportunity to make important and complex assessments of rapidly evolving cybersecurity situations. There is some risk that time-pressured disclosures may be overly broad and generic, and may be more misleading than informative. Corporate officers may need to make multiple amendments to disclose information about dynamic and sensitive situations. This may distract corporate stakeholders rather than allowing them to focus on addressing and remediating a significant cybersecurity incident, particularly to the extent that the disclosure prompts further attacks, regulatory investigations or private litigation, or inquiries from customers or counterparties.

Commissioner Hester M. Peirce highlighted many of these concerns in her statement regarding the Final Rules. There, she expressed concern that the "granular disclosures" prescribed by the Final Rules may help hackers more than investors. Commissioner Peirce said the Final Rules look like a "compliance checklist for handling cyber risk," which may serve to drive companies to spend resources on compliance than on combatting cyber threats. Commissioner Peirce also criticized the narrow law enforcement exception to the four-day reporting requirement, stating that "obtaining approval within four days will be quite a feat."

Preparation for Novel Disclosure. Companies, particularly calendar year-end companies, should begin drafting the section of their annual reports disclosing company processes for assessing, identifying and managing material risks from cybersecurity threats. This is new disclosure that will likely be carefully reviewed by the SEC, investors, proxy advisors and other stakeholders. Therefore, companies should allow ample time for officers and employees from various departments within their organizations and outside advisers to prepare, evaluate and revise these descriptions and have them reviewed by the Board of Directors or appropriate Board committee.

Reassess Processes. Companies should consider and review their cybersecurity processes in light of the new disclosure requirements and adjust their practices and policies accordingly in order to meet the applicable timelines. As they consider what they will be disclosing in light of the SEC's new cybersecurity disclosure rules, companies should reflect whether or not it would be advisable to make any substantive changes in how they handle cybersecurity matters. For example, does the company have employees, contractors or consultants with adequate cybersecurity expertise to evaluate if sufficient safeguards are in place? Does the company have mitigation plans in place that can be readily implemented? Is sufficient information being reported to the Board of Directors for it to provide oversight of cybersecurity matters? While the SEC's rules do not mandate specific policies, disclosures could result in investor feedback that may ultimately lead to changes in practices.

The Final Rules Do Not Prescribe Company Policy. In evaluating company policy, one should appreciate that the SEC stresses that companies must set their own policies in this area and not view the SEC's disclosure rules as prescribing company policies or even influencing them. For example, the SEC states: "[W]e confirm that the purpose of the rules is . . . to inform investors, not to influence whether and how companies manage their cybersecurity risk" and that the SEC seeks "to foreclose any perception that the rule prescribes cybersecurity policy."

No SEC Imposition on Corporate Boards. When considering director skills and board matrixes, note that the SEC dropped its proposal to require disclosure of board cybersecurity expertise, by crediting numerous concerns raised in the comment letters, including:

> (1) that "cybersecurity risk is not intrinsically different from other risks that directors assess with or without specific technical expertise," (2) such a "disclosure requirement would [unduly] pressure companies to retain cybersecurity experts on their board," (3) "identified expert directors would face elevated risks, such as being targeted by nation states for surveillance or hackers attempting to embarrass them," and (4) such a disclosure rule is "overly prescriptive."

The SEC said:

> "We are persuaded that effective cybersecurity processes are designed and administered largely at the management level, and that directors with broad-based skills in risk management and strategy often effectively oversee management's efforts without specific subject matter expertise, as they do with other sophisticated technical matters."

Of course, companies may choose to highlight applicable Board-level cybersecurity expertise if they wish, though it seems prudent to bear in mind the cautions expressed in the comment letters, which the SEC cites.

See the Final Rules and the related Fact Sheet and SEC announcement.

For more information about the topics discussed in this Legal Update, please contact any of the following authors.

Lawrence A. Cunningham
+1 212 506 2203
lcunningham@mayerbrown.com

Edward S. Best
+1 312 701 7100
ebest@mayerbrown.com

Rajesh De
+1 202 263 3366
rde@mayerbrown.com

Marc Leong
+1 212 506 2468
mleong@mayerbrown.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

Anna T. Pinedo
+1 212 506 2275
apinedo@mayerbrown.com

Laura D. Richman
+1 312 701 7304
lrichman@mayerbrown.com

Dominique Shelton Leipzig
+1 213 229 5152
dsheltonleipzig@mayerbrown.com

The Free Writings & Perspectives, or FW&Ps, blog provides news and views on securities regulation and capital formation. The blog provides up-to-the-minute information regarding securities law developments, particularly those related to capital formation. FW&Ps also offers commentary regarding developments affecting private placements, mezzanine or "late stage" private placements, PIPE transactions, IPOs and the IPO market, new financial products and any other securities-related topics that pique our and our readers' interest. Our blog is available at: www.freewritings.law.

ENDNOTES

[1] *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216; 34-97989; File No. S7-09-22 (Jul. 26, 2022), available at https://www.sec.gov/files/rules/final/2023/33-11216.pdf ("Adopting Release")

[2] See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038; 34-94382; IC-34529; File No. S7-09-22 (Mar. 9, 2022), available at https://www.sec.gov/files/rules/final/2023/33-11038.pdf ("Proposing Release")

[3] See EY CTR FOR BD. MATTERS, *How Cyber Governance and Disclosures are Closing the Gaps in 2022* (Aug. 2022), available at https://www.ey.com/en_us/board-matters/how-cyber-governance-and-disclosures-are-closing-the-gaps-in-2022.

[4] The Proposed Rules required the following to be disclosed: when the incident was discovered and whether it is ongoing; a brief description of the nature and scope of the incident; whether any data was stolen, altered, accessed or used for any other unauthorized purpose; the effect of the incident on the registrant's operations; and whether the registrant has remediated or is currently remediating the incident.

[6] The SEC's decision to exempt asset-backed issuers with no directors and officers from the Final Rules means that no amendment to Form SF-3 was required.