Milbank

Insights

Global Capital Markets Group

SEC Adopts Cybersecurity Rules and Reporting Requirements for Public Companies

August 2023

On July 26, 2023, the SEC adopted rules requiring public companies and foreign private issuers (i) to timely disclose material cybersecurity incidents and (ii) to disclose on an annual basis the registrant's cybersecurity risk management, strategy and governance. The SEC issued its rule proposal in March 2022, which was the subject of significant public commentary. As a result, the SEC made certain changes to the required disclosures, streamlining them to decrease the amount of detail needed. Yet, the final rule still dramatically alters the disclosure landscape for domestic and foreign registrants. Set forth below is a summary of the key provisions of the final rule.

I. Disclosure of Material Cybersecurity Incidents on Form 8-K

The adopted rules amend Form 8-K to add Item 1.05, requiring a registrant to disclose a cybersecurity incident within four business days after determining the incident is material.

Cybersecurity Incident. The final rule defines a "cybersecurity incident" broadly to include any "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." This differs from the proposed rule as it adds the "series of related unauthorized occurrences" language to ensure that companies report multiple incidents which are only material in the aggregate. For example, a bad actor may engage in multiple small cyberattacks which only when viewed together are material, or multiple bad actors may attack the same vulnerability which collectively cause an issue for the company.

Required Disclosure. Item 1.05 of Form 8-K requires that the following information be provided regarding a material cybersecurity incident:

- 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 proposed rule originally required additional information such as the incident's remediation status, whether it is ongoing, and whether data was compromised. However, these were removed to balance concerns that such detailed information could exacerbate security threats. In the same vein, the rule clarifies that a registrant need not provide "specific information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident."

Following the theme of reducing the amount of disclosure required by the proposed rule, the SEC removed much of the mandate for updates on reported cybersecurity incidents. The proposed rule required "any material changes, additions, or updates" on previously reported cybersecurity incidents to be discussed on the registrant's Form 10-Q or Form 10-K. Instead of the proposed formulation, the SEC now only requires updated disclosures on a Form 8-K amendment for information that is not determined or is unavailable at the time of the initial Item 1.05 report.

Timing. The registrant must make the required Item 1.05 disclosures within four business days of their determination that an incident is material. The final rule adopts the conventional definition of materiality:

"information is material if there is a substantial likelihood that a reasonable shareholder would consider it important." A materiality determination must be made without unreasonable delay, which is a departure from the proposed rule's "as soon as reasonably practicable." This change was meant to address the concern that companies could be forced to make materiality conclusions without sufficient information.

Exceptions. The final rule allows a registrant to delay disclosure in two scenarios. First, a registrant may delay up to 60 days if the Attorney General determines that it poses a substantial risk to national security or public safety. However, this exception does not provide a means for foreign regulators to delay disclosure for their own national security concerns. Second, if the company is subject to the FCC's customer proprietary network information rules, then the company must delay disclosure up to 7 days after notifying the FBI of an incident involving such information.

Limited Safe Harbor. The SEC has long held the view that a safe harbor is appropriate if the triggering event for the Form 8-K disclosure requires management to make a rapid materiality determination. In line with this view, the SEC adopted a safe harbor for Item 1.05 providing that (i) a failure to file the disclosure would not be deemed a violation of Section 10(b) and Exchange Act Rule 10b-5 and (ii) untimely filing would not result in a loss of Form S-3 eligibility.

Foreign Private Issuers. The SEC established cybersecurity incident disclosure requirements for foreign private issuers' ("FPIs") that mirror those for domestic issuers. The SEC's justification being that an FPI's cybersecurity incident is no less important to investors than a domestic registrants'. As such, FPIs must timely disclose material cybersecurity incidents on their Form 6-K.

II. Disclosure of Cybersecurity Risk Management, Strategy and Governance on Form 10-K

The adopted rules also amend Regulation S-K to add Item 1.06, which mandates that registrants provide a description of their cybersecurity risk management processes and governance structure on their Form 10-K.

Cybersecurity Risk Management and Strategy. Under the new Item 1.06(b), registrants are required to disclose their cybersecurity risk management processes. Specifically, they must discuss the processes for "assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes." Sticking with the goal of avoiding a level of detail that would advantage bad actors, the SEC replaced the proposed rule's "policies and procedures" with "processes". The final rule also adds a materiality qualifier to "risks", instead of listing proposed risk types, in order to be clear it is not prescribing cybersecurity policy.

Cybersecurity Governance. The new Item 1.06(c) mandates that the registrant describe their cybersecurity governance structure, including:

- the Board of Directors' oversight of material risks from cybersecurity threats,
- any board committee responsible for such oversight, and
- the processes by which the Board or committee is informed of such risks.

This is a less detailed disclosure than the proposed rule as it no longer requires (i) how the board integrates cybersecurity into its business strategy, risk management, and financial oversight or (ii) the frequency of board discussions on cybersecurity. Moreover, the proposed rule did not have a materiality qualifier for risks, the addition of which serves to cut down on the level of disclosure as well. Further, the SEC did not adopt the proposed rule requiring disclosure of the cybersecurity expertise of any board members. Their reasoning being that investors can form sound investment decisions without knowing board-level expertise.

Foreign Private Issuers. Form 20-F is amended by the final rule to include the same disclosure items required by Item 1.06 of Regulation S-K. Thus, FPIs must discuss their cybersecurity risk management, strategy, and government structure on their annual Form 20-F.

III. Effective Date

Effective Date for Item 1.05 of Form 8-K. The final rule becomes effective 30 days after its publication in the Federal Register. All registrants, except smaller reporting companies, are expected to comply with Item 1.05 of Form 8-K by the later of 90 days after the rules' publication or December 18, 2023. Smaller reporting companies are allowed an additional 180 days from the above compliance date to begin complying with Item 1.05.

Effective Date for Item 1.06 of Regulation S-K. The final rule becomes effective 30 days after its publication in the Federal Register. All registrants must comply with Item 1.06 of Regulation S-K beginning with annual reports for fiscal years ending on or after December 15, 2023.

Inline XBRL. All of these new disclosure requirements must be tagged in Inline XBRL, including by block text tagging narrative disclosures and detail tagging quantitative amounts. Registrants have an additional year after the disclosure compliance deadline to comply with the tagging requirement.

Global Capital Markets Group Contacts

New York	55 Hudson Yards, New York, NY 10001	
Carlos Albarracin	CAlbarracin@milbank.com	+1 212.530.5116
Paul Denaro	PDenaro@milbank.com	+1 212.530.5431
Antonio Diaz-Albertini	ADiaz-Albertini@milbank.com	+1 212.530.5002
Jonathon Jackson	JJackson@milbank.com	+1 212.530.5503
Lesley Janzen	LJanzen@milbank.com	+1 212.530.5890
Rod Miller	RDMiller@milbank.com	+1 212.530.5022
Marcelo Mottesi	MMottesi@milbank.com	+1 212.530.5602
Brett Nadritch	BNadritch@milbank.com	+1 212.530.5301

Please feel free to discuss any aspects of this Client Alert with your regular Milbank contacts or any member of our Global Capital Markets Group.