Tucker Ellis LLP

# SEC Adopts Final Cybersecurity Disclosure Rules

**AUGUST 2023**

On July 26, 2023, the Securities and Exchange Commission ("SEC"), by a 3-2 vote, approved new disclosure rules designed to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934.

The SEC cited a number of reasons for the adoption of the new rules, stemming from investors' and other capital markets participants' need for more timely and reliable information related to companies' cybersecurity due to:

- an ever-increasing share of economic activity dependent on electronic systems, such that disruptions to those systems can have significant effects on companies;
- the substantial rise in the prevalence of cybersecurity incidents, propelled by several factors: the increase in remote work spurred by the COVID-19 pandemic; the increasing reliance on third-party service providers for information technology services; and the rapid monetization of cyberattacks facilitated by ransomware, black markets for stolen data, and crypto-asset technology; and
- increasing costs and adverse consequences of cybersecurity incidents to companies, including business interruption, lost revenue, ransom payments, remediation costs, liabilities to affected parties, cybersecurity protection costs, lost assets, litigation risks, and reputational damage.

The new rules require (i) current disclosure on Form 8-K about material cybersecurity incidents, and (ii) periodic disclosure on Form 10-K about a company's processes to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks.

> ***Cybersecurity incident*** means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

**Form 8-K**

**Beginning on December 18, 2023**, new Item 1.05 of Form 8-K (Material Cybersecurity Incidents) requires disclosure if a company experiences a material cybersecurity incident. The disclosure requires a company 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 company, including its financial condition and results of operations. The filing deadline (similar to other Form 8-K items) is four business days after the filing trigger, which is the date that a company has developed information regarding an incident sufficient for a company to make a materiality determination. Instruction I to new Item 1.05 provides that "[a] registrant's materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident." The disclosure may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing.

The SEC has advised that the materiality determination should be consistent with that set out in the numerous cases addressing materiality in the securities laws that hold, in summary, 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." The SEC's adopting release further clarifies that companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident.

**Form 10-K**

Form 10-K has been amended, **beginning with Form 10-Ks for fiscal years ending after December 15, 2023**, to require new disclosures related to cybersecurity under new Regulation S-K Item 106. New Item 106 requires companies to describe their processes, if any, 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 company. New Item 106 also requires companies to describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

In providing such disclosure, companies should address, as applicable, the following non-exclusive list of disclosure items:

- Whether and how any such 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 such risks from cybersecurity threats associated with its use of any third-party service provider.

Companies also are required to (i) describe 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 company, including its business strategy, results of operations, or financial condition, and, if so, how; (ii) if applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats, and describe the processes by which the board or such committee is informed about such risks; and (iii) describe management's role in assessing and managing the company's material risks from cybersecurity threats, and, as applicable, the following non-exclusive 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 of directors or a committee or subcommittee of the board of directors.

The final rules require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language ("Inline XBRL") beginning one year after the initial compliance with the related disclosure requirement.

Smaller reporting companies will have an additional 180 days and must begin complying with Form 8-K Item 1.05 on the later of 270 days from the effective date of the rules or June 15, 2024.

**Practice Pointers**

For companies on a calendar year cycle, the compliance dates will come quickly. Companies should review the new cybersecurity disclosures rules with their Chief Technology Officer and/or Chief Information Officer and other appropriate senior leadership and evaluate – and upgrade, if necessary – their processes and procedures for addressing cybersecurity incidents. Companies should review their disclosure controls and procedures to ensure that appropriate members of company management are timely informed of cybersecurity incidents to make materiality determinations without unreasonable delay. Companies should

develop a plan to respond to cybersecurity incidents and make the appropriate disclosure related to material cybersecurity incidents. Finally, companies also should review their current cybersecurity management and governance to address the new disclosure rules.

## Additional Information

For more information, please contact:


- Robert M. Loesch | 216.696.5916 | robert.loesch@tuckerellis.com
- Glenn E. Morrical | 216.696.3431 | glenn.morrical@tuckerellis.com
- Kristen A. Baracy | 213.430.3603 | kristen.baracy@tuckerellis.com