CYBERSECURITY LAW ALERT

July 28, 2023

By: Andrew T. Garbarino, Esq.
Nicole E. Osborne, Esq.

RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.

Four Days to Report:
The SEC Tightens Cybersecurity Reporting Requirements for Public Companies

This week, the U.S. Securities and Exchange Commission (SEC) narrowly (by a 3-2 margin) voted to approve rules mandating that public companies report cyber incidents and to disclose, on an annual basis, material information regarding a company's cybersecurity risk management, strategy and governance. These new rules shift the way public companies must react to data breaches and manage its reporting.

The new data breach reporting requirement stems from the fact that cyber incidents may be "material to investors", as stated by SEC chair Gary Gensler. The rules will require companies to report significant cyber incidents on Form 8-K (under new Item 1.05) filed with the SEC ***within four business days*** of a public company determining that a cyber incident will have a material impact. The resultant 8-K filing would require disclosure of the scope, nature, and timing of the incident, as well as the potential of civil litigation or government investigations and proceedings, and harm to the company's reputation or its relationships with customers and vendors. Item 1.05 will also require a recitation of the board's oversight of cyber risks.

There is one narrow exception to the four-day reporting requirement. In the event that the reporting of an incident might create "significant" national-security or public safety issues, the reporting may be delayed for up to thirty (30) days upon written request by the U.S. Attorney General, which in-turn may be extended upon additional requests.

The materiality aspect looks to be the obvious battleground when it comes to the SEC's enforcement of potential violations. While it remains to be seen exactly how the SEC will interpret and implement the materiality of a cyber incident, public companies must immediately begin to prepare for how they will respond to potential cyber incidents in the future. Businesses should have a plan in place to address how and when materiality will be determined.

The four-day reporting mandate is concerning for public entities as it may cause businesses to make public reports of a cyber incident before the company has sufficient understanding of the nature of an incident. Moreover, the disclosure may be required prior to any remediation efforts taking place, further leaving a company's system vulnerable to cyber-attacks.

The approved rules also add Regulation S-K Item 106, requiring companies to describe their processes for assessing, identifying and managing material cyber risks, as well as describing the potential material effects that an incident may have.

The SEC removed portions from its initially proposed rules that would have required certain technical details in the filing, to avoid potentially worsening cyber incidents by disclosing such information. Even with such removal, companies will still be required to describe procedures and protocols relating to the identification of material cybersecurity risks in their annual reports.

Another section removed from the proposed rules was the identification of board members with cybersecurity expertise. The removal of that requirement does not mean that a company should not seek out board members with strong cybersecurity backgrounds, which are certainly worthwhile in this landscape. However, the rules do require disclosure of the cybersecurity acumen of management-level employees.

Compliance with the cyber incident-reporting mandate is effective as of December 18, 2023. Compliance with the annual reporting mandate begins on December 15, 2023 for large business and June 15, 2024 for smaller companies.

These new rules cement the importance of cybersecurity as part of the mission of the SEC, and it is expected that additional rules and regulations will come in the near future. Considering the breadth of state and other federal agency rules, cyber compliance is becoming all the more complicated. Ruskin Moscou Faltischek will continue to monitor the status of this new rule and any other regulation or enforcement proceedings that may follow. If you have any questions regarding this new rule or any other cybersecurity related questions, please contact:

Andrew T. Garbarino, Esq.
516.663.6632
agarbarino@rmfpc.com

Nicole E. Osborne, Esq.
516.663.6687
nosborne@rmfpc.com