Governance & Securities Alert

Weil

From the Public Company Advisory Group of Weil, Gotshal & Manges LLP

December 13, 2023

SEC Cybersecurity Incident Disclosure Requirements Begin December 18, 2023

- DOJ publishes guidelines for when disclosure would pose a substantial risk to national security or public safety
- FBI recommends companies establish a relationship with the cyber squad at their local FBI field office
- Controls and Procedures need to be in place

By Howard Dicker and Olivia Greer

As we previously discussed in greater detail, earlier this year the U.S. Securities and Exchange Commission adopted cybersecurity disclosure rules that require a U.S. public company to disclose (1) on Form 8-K (Item 1.05) the occurrence of a material cybersecurity incident within four business days after determining that such incident is material and (2) in the Annual Report on Form 10-K (Item 1C), the company's risk management, strategy and governance of cybersecurity. Foreign private issuers (FPIs) are subject to similar requirements.

Most companies must begin complying with the incident disclosure requirements on Forms 8-K and 6-K (for FPIs) on December 18, 2023. Smaller reporting companies must comply with these requirements by June 15, 2024. All companies must comply with the risk management, strategy and governance disclosure beginning with annual reports for the fiscal year ending on or after December 15, 2023. Inline XBRL is required one year after the initial compliance date for the related disclosure requirement.

The filing of a Form 8-K for a material cybersecurity incident may be delayed for a limited period of time if the U.S. Attorney General determines that disclosure would pose a substantial risk to national security or public safety and notifies the SEC in of such determination in writing. On December 12, 2023, the Department of Justice published guidelines outlining the process that companies (or U.S. Government agencies in coordination with such companies) may use to request that the DOJ authorize such delays. When a company discovers a cybersecurity incident and believes that disclosure may pose a substantial risk to national security or public safety, the company should, directly or through another U.S. Government agency (e.g., the U.S. Secret Service, another federal law enforcement agency, the Cybersecurity & Infrastructure Security Agency (CISA), or another sector risk management agency (SRMA)), immediately contact the Federal Bureau of Investigation consistent with reporting instructions the FBI recently issued. According to the guidelines, it is important that the company provide the FBI, directly or indirectly through another U.S. Government agency, information about a cybersecurity incident likely to meet the requirements for delayed disclosure as soon as possible, even beginning well before the company has completed its materiality analysis or its investigation into the incident.[1]

[1] This is because the Attorney General must notify the SEC in writing of its determination to invoke the delay prior to the four business day Form 8-K filing deadline. Also on December 12, 2023, the SEC staff issued three Form 8-K CDIs relating to requests to the Attorney General. For example, one CDI stresses that requesting a delay does not change a company's filing obligation. If the Attorney General declines to make a determination or does not respond before the Form 8-K otherwise would be due, the company still is obligated to file the Item 1.05 Form 8-K within four business days of the company's determination that the incident was material.

Invoking a Form 8-K filing delay will be difficult. At the time the SEC adopted the new rules, SEC Commissioner Peirce expressed skepticism that approval could be obtained from the Attorney General within the four business days, stating that it would be "quite a feat" and noting that the rule makes extensions of the delay beyond the initial 30 days difficult. Moreover, the DOJ guidelines state that:

> The primary inquiry for the DOJ is whether the *public disclosure* of a cybersecurity incident threatens public safety or national security, not whether the incident itself poses a substantial risk to public safety and national security. While cybersecurity incidents themselves frequently threaten public safety and national security, the disclosure to the public that those incidents have occurred poses threats less often. In many circumstances, the prompt public disclosure of relevant information about a cybersecurity incident provides an overall benefit for investors, public safety, and national security.

We expect that most companies in the face of most incidents will find a Form 8-K filing delay unavailable. Pursuing one is likely to consume time and resources that companies may conclude are better spent on addressing the breach and related matters. Furthermore, maintaining legal privilege will be difficult once a company provides information to the FBI or other U.S. Government agency.

Preparation is important. Significant cybersecurity incidents are themselves challenging and raise a multitude of issues. Recently the FBI recommended that all publicly traded companies establish a relationship with the cyber squad at their local FBI field office. The SEC rules demand that companies have appropriate incident response processes in place. We highlight this in our previous alert, describing for companies "What to Do Now?" Moreover, in recent years SEC enforcement has actively pursued companies that fail to adopt and implement adequate controls and procedures related to cybersecurity.

* * *

If you have questions concerning the contents of this Alert, or would like more information, please speak to your regular contact at Weil or to any of the following authors:

Authors

Howard B. Dicker	View Bio	howard.dicker@weil.com	+1 212 310 8858
Olivia J. Greer	View Bio	olivia.greer@weil.com	+1 212 310 8815