Articles + Publications | May 31, 2024

Director of Division of Corporation Finance Issues Guidance on Disclosure of Cybersecurity Incidents under Form 8-K

WRITTEN BY

David I. Meyers | Sadia Mirza | Seth A. Winter | Danilo P. Castelli

On May 21, 2024, Erik Gerding, the director of the Division of Corporation Finance of the Securities and Exchange Commission (SEC), released a statement containing guidance for public companies regarding the disclosure of material cybersecurity incidents under Item 1.05 of Form 8-K. In July 2023, the SEC adopted final rules to require more immediate disclosure of material cybersecurity incidents by public companies. The final rules added Item 1.05 to Form 8-K, which, effective December 2023, requires public companies to disclose any cybersecurity incident within four business days after it is determined to be material.

In his statements, Gerding commented that since the new rules became effective, there has been a growing trend of companies voluntarily disclosing cybersecurity incidents under Item 1.05 of Form 8-K prior to making a materiality determination with respect to such cybersecurity incidents. Gerding pointed out that although the text of Item 1.05 does not expressly prohibit voluntary disclosure, Item 1.05 was added to Form 8-K to require the disclosure of a cybersecurity incident that is determined by a registrant to be material (Item 1.05 is after all titled "Material Cybersecurity Incidents). The director clarified that while voluntary disclosure of cybersecurity incidents that are immaterial or for which a materiality determination has not yet been made is still encouraged, that disclosure should be made under a different item of Form 8-K — for example, under Item 8.01. The director believes it may be confusing for investors when companies disclose immaterial cybersecurity incidents or incidents for which a materiality determination has not yet been made under Item 1.05, where the heading includes the word "material."

Choosing to voluntarily file under Item 8.01 of Form 8-K instead of Item 1.05 can offer an issuer two key strategic benefits. First, Item 8.01 allows for a more flexible filing timeline and is not subject to the same four-business day filing deadline as an event required to be disclosed under Item 1.05 (note that separate filing timelines may apply, including if the issuer is seeking to satisfy an obligation under Regulation FD). Second, such a voluntary filing reduces the burden of disclosure, as Item 8.01 does not require the same level of detail regarding a cybersecurity event as Item 1.05 of Form 8-K.

Gerding further noted that, given the prevalence of cybersecurity incidents, distinguishing between material cybersecurity incidents required to be disclosed under Item 1.05 and immaterial cybersecurity incidents (or incidents where a company has not yet made a materiality determination) voluntarily disclosed under Item 8.01 will permit investors to more easily distinguish between the two and allow investors to make better investment and voting decisions with respect to material cybersecurity incidents.

Gerding also provided further guidance on cybersecurity disclosure under Item 1.05 of Form 8-K:

- If a company discloses an immaterial incident (or one for which it has not yet made a materiality determination) under Item 8.01 of Form 8-K, and then it subsequently determines that the incident is material, it should then file an Item 1.05 Form 8-K within four business days of such materiality determination. Although the subsequent filing may refer to the Item 8.01 Form 8-K, companies must ensure that the subsequent filing satisfies the requirements of Item 1.05 of Form 8-K.

- In instances where a cybersecurity incident is so significant that a company determines it to be material even though it has not yet determined its actual impact (or reasonably likely impact), such company should disclose the incident under Item 1.05 of Form 8-K to provide investors with information necessary to understand the material aspects of the nature, scope and timing of the cybersecurity incident and should include a statement noting that the company has not yet determined the impact of the incident. Companies should subsequently amend the Form 8-K to disclose the impact of the incident within four business days either after the registrant, without unreasonable delay, determines such information or after that information becomes available.

Gerding's statement reminded companies that in analyzing a cybersecurity incident for materiality, and in assessing an incident's impact (or reasonably likely impact), companies should assess all relevant factors, including, but not limited to, the impact on "financial condition and results of operations," and other qualitative factors as well, such as whether the incident will harm a company's reputation, customer or vendor relationships or competitiveness, and the possibility of domestic or foreign litigation or regulatory investigations or actions. As with any materiality determination, companies should conduct proper diligence as part of the materiality analysis and should consider documenting the factors considered as part of the ultimate materiality determination in the event company auditors or the SEC staff were to raise any questions with respect to a company's disclosure.

For additional information on the SEC's cybersecurity disclosure rules, see our alert here.

RELATED INDUSTRIES + PRACTICES

- Capital Markets
- Corporate
- Corporate Governance
- Data + Privacy
- Privacy + Cyber