May 24, 2024

SEC Staff Clarifies Form 8-K Reporting Requirements for Cyber Incidents

On May 21, 2024, the SEC's Director of the Division of Corporation Finance, Erik Gerding, published a statement urging public companies to report only material cyber incidents under the SEC's new cybersecurity rules. Those rules, which the SEC adopted in July 2023 and went into effect for most companies on December 18, 2023, require public companies to disclose material cybersecurity incidents under new Item 1.05 of Form 8-K. When adopting the new rules, the Commission stated that Item 1.05 "is not triggered until the company determines the materiality of an incident." Notwithstanding that guidance, many of the disclosures made under Item 1.05 in the five months since the rule took effect have included statements that the company making the disclosure has not yet determined that the incident is material or, in some cases, has determined that the incident is not material. Although acknowledging that such disclosures are not expressly prohibited by the text of Item 1.05, Gerding warns that disclosing such immaterial (or not yet material) incidents under Item 1.05 "could be confusing for investors," and he encourages companies to disclose such incidents under a different item of Form 8-K, such as Item 8.01 (Other Events).

Background: The July 2023 Rule on Reporting Material Cyber Incidents

Item 1.05 of Form 8-K requires specified disclosure of material cybersecurity incidents. Whether a cybersecurity incident is material is determined by the same materiality principles articulated repeatedly by the courts and the SEC – namely whether there is a substantial likelihood that a reasonable investor would consider it important.

Gerding reminds companies that the materiality assessment "should not be limited to the impact on 'financial condition and results of operation,' and 'companies should consider qualitative factors alongside quantitative factors.' For example, companies should consider whether the incident will 'harm . . . [its] reputation, customer or vendor relationships, or competitiveness.' Companies should also consider 'the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and Federal Government authorities and non-U.S. authorities.'"

Under Item 1.05 of Form 8-K, companies must, within four business days of their determination that a "material cybersecurity incident" has occurred, file a Form 8-K describing 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. If any information required by Item 1.05 is not determined or unavailable at the time the Form 8-K filing is required, companies must file an amendment to the Form 8-K to include such disclosure within four business days of determination or availability.

Clarification: Reporting Incidents That Are Immaterial or for Which a Company Has Not Yet Made a Materiality Determination

While the SEC may have expected Item 1.05 to be used only to report material cyber incidents, in the five months since the rule took effect more than a dozen companies have disclosed incidents under Item 1.05 that the companies have not yet determined are material—and therefore do not require disclosure under Item 1.05. This unexpected practice has resulted in an increase in the overall number of Form 8-K disclosures regarding cybersecurity incidents. But because Item 1.05 was added to Form 8-K to require the disclosure of a cybersecurity incident "that is determined by the registrant to be material," and, in fact, the item is titled "Material Cybersecurity Incidents," Gerding suggests that "it could be confusing for investors if companies disclose either immaterial cybersecurity incidents or incidents for which a materiality determination has not yet been made under Item 1.05."

Gerding does not suggest that such incidents should not be disclosed. He "recognize[s] the value of such voluntary disclosures to investors, the marketplace, and ultimately to companies, and [his] statement is not intended to disincentivize companies from making those disclosures." Rather, his statement is intended to encourage companies to report immaterial incidents under a different item of Form 8-K, not Item 1.05:

> Given the prevalence of cybersecurity incidents, this distinction between a Form 8-K filed under Item 1.05 for a cybersecurity incident determined by a company to be material and a Form 8-K voluntarily filed under Item 8.01 for other cybersecurity incidents will allow investors to more easily distinguish between the two and make better investment and voting decisions with respect to material cybersecurity incidents. By contrast, if all cybersecurity incidents are disclosed under Item 1.05, then there is a risk that investors will misperceive immaterial cybersecurity incidents as material, and vice versa.

Takeaways

Public companies should carefully consider the specific item of Form 8-K under which they disclose cybersecurity incidents. Since Item 1.05 was added, many companies have erred on the side of providing early disclosure under Item 1.05 even before the company has determined that an incident is material. Gerding acknowledges that early, voluntary disclosures have value to investors and the marketplace. But his statement is a reminder that such early disclosures are not the end of the analysis. Even if a company made an early disclosure, once it determines that an incident is material the company is required to disclose the material impact of the incident in a subsequent filing that satisfies all of the requirements of Item 1.05.

Companies can expect the SEC to vigorously enforce disclosure requirements related to cybersecurity incidents. Just this week Intercontinental Exchange Inc., the parent company of the New York Stock Exchange, agreed to pay a $10 million penalty to settle allegations that it failed to comply with its obligation under a different rule (Regulation Systems Compliance and Integrity, or Regulation SCI) to immediately notify the SEC of an April 2021 cybersecurity incident. The Commission also continues to prosecute its complaint against SolarWinds Corp. and the company's Chief Information Security Officer for allegedly misleading disclosures in December 2020 about a cybersecurity incident. These enforcement actions, considered alongside the new disclosure rules and efforts by Gerding and other staff to engage with industry regarding these rules, signal the SEC's commitment to aggressively policing companies' cybersecurity disclosures.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jonathan H. Ashtor
+1-212-373-3823
jashtor@paulweiss.com

L. Rush Atkinson
+1-202-223-7473
ratkinson@paulweiss.com

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Lina Dagnew
+1-202-223-7455
ldagnew@paulweiss.com

David S. Huntington
+1-212-373-3124
dhuntington@paulweiss.com

Luke Jennings
+1-212-373-3591
ljennings@paulweiss.com

Christodoulos Kaoutzanis
+1-212-373-3445
ckaoutzanis@paulweiss.com

Raphael M. Russo
+1-212-373-3309
rrusso@paulweiss.com

Peter Carey
+1-202-223-7485
pcarey@paulweiss.com

Anna R. Gressel
+1-212-373-3388
agressel@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com