Blogs

In recent weeks, Corp Fin has been active in providing guidance about Form 8-Ks filed to report cyber incidents. Corp Fin Director Erik Gerding has issued **two separate statements** – and now Corp Fin has issued five CDIs. These CDIs are in addition to the **Item 1.05 guidance** that was released near the end of the year by the SEC and the DOJ.

For the most part, the new CDIs address Form 8-Ks filed in the wake of ransomware attacks. These CDIs specifically are:

Question 104B.05

Question: A registrant experiences a cybersecurity incident involving a ransomware attack. The ransomware attack results in a disruption in operations or the exfiltration of data. After discovering the incident but before determining whether the incident is material, the registrant makes a ransomware payment, and the threat actor that caused the incident ends the disruption of operations or returns the data. Is the registrant still required to make a materiality determination regarding the incident?

Answer: Yes. Item 1.05 of Form 8-K requires a registrant that experiences a cybersecurity incident to determine whether that incident is material. The cessation or apparent cessation of the incident prior to the materiality determination, including as a result of the registrant making a ransomware payment, does not relieve the registrant of the requirement to make such materiality determination.

Further, in making the required materiality determination, the registrant cannot necessarily conclude that the incident is not material simply because of the prior cessation or apparent cessation of the incident. Instead, in assessing the materiality of the incident, the registrant should, as the Commission noted in the adopting release for Item 1.05 of Form 8-K, determine "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," notwithstanding the fact that the incident may have already been resolved. *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release Nos. 33-11216; 34-97989 (July 26, 2023) [88 FR 51896, 51917 (Aug. 4, 2023)] (quoting *Matrixx Initiatives v. Siracusano*, 563 U.S. 27, 38-40 (2011); *Basic Inc. v. Levinson*, 485 U.S. 224, 240 (1988); *TSC Indus. v. Northway*, 426 U.S. 438, 449 (1976)) (internal quotation marks omitted). [June 24, 2024]

Question 104B.06

Question: A registrant experiences a cybersecurity incident that it determines to be material. That incident involves a ransomware attack that results in a disruption in operations or the exfiltration of data and has a material impact or is reasonably likely to have a material impact on the registrant, including its financial condition and results of operations. Subsequently, the registrant makes a ransomware payment, and the threat actor that caused the incident ends the disruption of operations or returns the data. If the registrant has not reported the incident pursuant to Item 1.05 of Form 8-K before it made the ransomware payment and the threat actor has ended the disruption of operations or returned the data before the Form 8-K Item 1.05 filing deadline, does the registrant still need to disclose the incident pursuant to Item 1.05 of Form 8-K?

Answer: Yes. Because the registrant experienced a cybersecurity incident that it determined to be material, the subsequent ransomware payment and cessation or apparent cessation of the incident does not relieve the registrant of the requirement to report the incident under Item 1.05 of Form 8-K within four business days after the registrant determines that it has experienced a material cybersecurity incident. [June 24, 2024]

Question 104B.07

Question: A registrant experiences a cybersecurity incident involving a ransomware attack, and the registrant makes a ransomware payment to the threat actor that caused the incident. The registrant has an insurance policy that covers cybersecurity incidents and is reimbursed for all or a substantial portion of the ransomware payment. Is the incident necessarily not material as a result of the registrant being reimbursed for the ransomware payment under its insurance policy?

Answer: No. The standard that the Commission articulated for assessing the materiality of a cybersecurity incident under Item 1.05 of Form 8-K is set forth in the adopting release for the rule and is reiterated in Question 104B.05. Further, as the Commission noted in the adopting release for Item 1.05 of Form 8-K, when assessing the materiality of cybersecurity incidents, registrants "should take into consideration all relevant facts and

circumstances, which may involve consideration of both quantitative and qualitative factors" including, for example, "consider[ing] both the immediate fallout and any longer term effects on its operations, finances, brand perception, customer relationships, and so on, as part of its materiality analysis." *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release Nos. 33-11216; 34-97989 (July 26, 2023) [88 FR 51896, 51917 (Aug. 4, 2023)]. Under the facts described in this question, such consideration also may include an assessment of the subsequent availability of, or increase in cost to the registrant of, insurance policies that cover cybersecurity incidents. [June 24, 2024]

Question 104B.08

Question: A registrant experiences a cybersecurity incident involving a ransomware attack. Is the size of the ransomware payment, by itself, determinative as to whether the cybersecurity incident is material? For example, would a ransomware payment that is small in size necessarily make the related cybersecurity incident immaterial?

Answer: No. The standard that the Commission articulated for assessing the materiality of a cybersecurity incident under Item 1.05 of Form 8-K is set forth in the adopting release for the rule and reiterated in Question 104B.05. Under that standard, the size of any ransomware payment demanded or made is only one of the facts and circumstances that registrants should consider in making its materiality determination regarding the cybersecurity incident. Further, in the adopting release for Item 1.05 of Form 8-K, the Commission declined "to use a quantifiable trigger for Item 1.05 because some cybersecurity incidents may be material yet not cross a particular financial threshold."

Any ransomware payment made is only one of the various potential impacts of a cybersecurity incident that a registrant should consider under Item 1.05. As the Commission further stated in Item 1.05's adopting release:

"[T]he material impact of an incident may encompass a range of harms, some quantitative and others qualitative. A lack of quantifiable harm does not necessarily mean an incident is not material. For example, an incident that results in significant reputational harm to a registrant . . . may not cross a particular quantitative threshold, but it should nonetheless be reported if the reputational harm is material."

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11216; 34-97989 (July 26, 2023) [88 FR 51896, 51906 (Aug. 4, 2023)]. [June 24, 2024]

Question 104B.09

Question: A registrant experiences a series of cybersecurity incidents involving ransomware attacks over time, either by a single threat actor or by multiple threat actors. The registrant determines that each incident, individually, is immaterial. Is disclosure of those cybersecurity incidents nonetheless required pursuant to Item 1.05 of Form 8-K?

Answer: Disclosure of those cybersecurity incidents may, depending on the particular facts and circumstances, be required pursuant to Item 1.05 of Form 8-K. In these circumstances, the registrant should consider whether any of those incidents were related, and if so, determine whether those related incidents, collectively, were material. The definition of "cybersecurity incident" under Item 106(a) of Regulation S-K (which, as noted in Instruction 3 to Item 1.05, is the definition that applies to Item 1.05 of Form 8-K) includes "a series of related unauthorized occurrences." In the adopting release for Item 1.05, the Commission noted:

"[W]hen a company finds that it has been materially affected by what may appear as a series of related cyber intrusions, Item 1.05 may be triggered even if the material impact or reasonably likely material impact could be parceled among the multiple intrusions to render each by itself immaterial. One example was provided in the

Proposing Release: the same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material. Another example is a series of related attacks from multiple actors exploiting the same vulnerability and collectively impeding the company's business materially."

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11216; 34-97989 (July 26, 2023) [88 FR 51896, 51910 (Aug. 4, 2023)]. [June 24, 2024]

Explore more in

Corporate Law

Topics

Quick Alerts
Blog series

Public Chatter

Public Chatter provides practical guidance—and the latest developments—to those grappling with public company securities law and corporate governance issues, through content developed from an in-house perspective.

View the blog