SEC Releases New Guidance on Material Cybersecurity Incident Disclosure

June 27, 2024

On June 24, 2024, the staff of the Division of Corporation Finance of the Securities and Exchange Commission (the "SEC") released five new Compliance & Disclosure Interpretations ("C&DIs") relating to the disclosure of material cybersecurity incidents under Item 1.05 of Form 8-K. A summary of the updates is below, followed by the full text of the new C&DIs. While the fact patterns underlying the new C&DIs focus on ransomware, issuers should consider the guidance generally in analyzing disclosure obligations for cybersecurity events.

ITEM 1.05 OF FORM 8-K

- *Completed ransomware attack does not absolve materiality determination:* The cessation or apparent cessation of the incident prior to the materiality determination does not necessarily indicate that the incident was not material, and the registrant still needs to make a determination. If a registrant experiences a cybersecurity incident involving a ransomware attack and, prior to any materiality determination by the registrant, the registrant pays the ransom and the threat actor ends their disruption of operations and returns any exfiltrated data, the registrant must still make a determination regarding the incident's materiality. (*Q&A 104B.05*)

- *Completed material cybersecurity event must still be disclosed:* A cybersecurity incident that a registrant determines to have had a material impact or that is reasonably likely to result in a material impact on the registrant must still be disclosed on a Form 8-K within four business days after the registrant makes a materiality determination, even if the cessation or apparent cessation of the incident occurs prior to the filing of the Form 8-K. (*Q&A 104B.06*)

- *Insurance coverage:* When determining whether a cybersecurity incident is material, reimbursement for a ransomware payment under a registrant's insurance policy does not mean that it is immaterial. Registrants must consider all relevant facts and circumstances, including both quantitative and qualitative factors such as the near-term and long-term effects on a registrant's operations, finances, brand perception, customer relationships, among other factors, when making a materiality determination. (*Q&A 104B.07*)

- *Amount of ransomware payment:* The size of the ransomware payment, by itself, is not determinative of whether a cybersecurity incident is material and is only one fact relevant to a registrant's materiality determination. (*Q&A 104B.08*)

- *Related immaterial cybersecurity events*: If a registrant experiences a series of cybersecurity incidents that, individually, are determined to be immaterial, the registrant should consider whether those prior incidents might be related, and if so related, determine whether the cybersecurity incidents, when viewed collectively, are material. In particular, the C&DIs highlight that Item 106(a) of Regulation S-K includes in the definition of cybersecurity incident "a series of related unauthorized occurrences." (*Q&A 104B.09*)

* * *

We are available to discuss these updates and other considerations related to cybersecurity incident disclosure. Please do not hesitate to contact us with any questions.

Eric T. Juergens
Partner, New York
+ 1 212 909 6301
etjuergens@debevoise.com

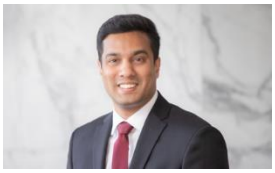
Erez Liebermann
Partner, New York
+ 1 212 909 6224
eliebermann@debevoise.com

Benjamin R. Pedersen
Partner, New York
+ 1 212 909 6121
brpedersen@debevoise.com

Paul M. Rodel
Partner, New York
+ 1 212 909 6478
pmrodel@debevoise.com

Anna Moody
Counsel, Washington, D.C.
+ 1 202 383 8017
amoody@debevoise.com

Kelly Donoghue
Associate, New York
+ 1 212 909 6145
kgdonoghue@debevoise.com



John Jacob
International Associate, New York
+ 1 212 909 6795
jjacob@debevoise.com

NEW AND UPDATED C&DIS:

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]