Articles + Publications | July 8, 2024

SEC Issues Additional Guidance Regarding Cybersecurity Incident Disclosure

WRITTEN BY

David I. Meyers | Danilo P. Castelli | DeJuawn "DJ" Griffin | Sadia Mirza

On June 24, the staff of the U.S. Securities and Exchange Commission's (SEC) Division of Corporation Finance (Division of Corporation Finance) released five new Compliance & Disclosure Interpretations (C&DIs) relating to the disclosure of material cybersecurity incidents under Item 1.05 of Current Reports on Form 8-K for situations involving ransomware payments. The new Item 1.05 C&DIs follow a recent enforcement action against R.R. Donnelley & Sons Company (RRD), pursuant to which RRD agreed to pay more than $2.1 million to settle charges related to inadequate disclosure and internal control failures concerning cybersecurity incidents that occurred in late 2021.

Additionally, on June 20, the director of the Division of Corporation Finance released a statement addressing concerns of cybersecurity incident disclosure and selective disclosure concerns under Regulation FD.

Below is a summary of the new C&DIs and the director's recent statement.

New Cybersecurity C&DIs

Question 104B.05

Question 104B.05 clarifies that a materiality determination is required in the context of a cybersecurity incident involving a ransomware attack that results in a disruption of operations or the exfiltration of data, even if the incident is resolved prior to the materiality determination because the issuer made a ransomware payment. The C&DI clarifies that even in such instances, a company must still assess the materiality of the cybersecurity incident and cannot necessarily conclude an incident is immaterial simply because it has concluded or appears to be concluded. Instead, in assessing the materiality of the incident, a company should 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.

Question 104B.06

Question 104B.06 focuses on a material ransomware situation where a company has made a ransomware payment, and the threat actor that caused the incident ends the disruption of operations or returns the data prior to the Item 1.05 Form 8-K filing deadline. The CD&I reiterates that an Item 1.05 Form 8-K filing is required within four business days after a company determines it has experienced a material cybersecurity incident. The CD&I clarifies

that because such company 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 a company of the requirement to report the incident under Item 1.05 of Form 8-K within four business days after the company determines that it has experienced a material cybersecurity incident. The Item 1.05 Form 8-K filing obligation remains even if the attack has ended or the data has been recovered through a ransom payment, prior to the Item 1.05 Form 8-K's due date.

Question 104B.07

Question 104B.07 clarifies that a materiality analysis is required even when a company has cybersecurity insurance policy that covers cybersecurity incidents. The staff clarified that an insurance policy covering all or a substantial part of a ransomware payment does not automatically render a cybersecurity incident immaterial. The C&DI emphasizes that companies must consider all relevant facts and circumstances in assessing materiality, including both quantitative and qualitative factors. This includes the immediate and long-term effects on operations, finances, brand perception, and customer relationships, and may also include an assessment of the subsequent availability of, or increase in cost to the company of, insurance policies that cover cybersecurity incidents.

Question 104B.08

Question 104B.08 clarifies that the size of a ransomware payment is only one factor in the materiality assessment of a cybersecurity incident and that it, by itself, is not a determinative factor of whether such incident is material. The staff also clarified that a small ransom payment does not necessarily mean that the related incident is immaterial and that companies should consider the overall context and impact of the incident, rather than relying solely on the amount paid, when determining materiality of the incident. As the Item 1.05 Adopting Release stated: "[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."[1]

Question 104B.09

Question 104B.09 addresses the scenario where a company experiences a series of individually immaterial cybersecurity incidents, either by a single threat actor or by multiple threat actors. The staff clarified that an Item 1.05 Form 8-K may be required depending on the particular facts and circumstances, and that a company should consider whether any of these incidents are related and, if so, assess whether the related events are cumulatively material. The CD&I underscores the need for a holistic view of related incidents to determine their collective materiality, even if each incident alone is not material. Two examples provided include: (i) if the same threat actor engages in several smaller but continuous cyberattacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material; and (ii) a series of related attacks from multiple actors exploiting the same vulnerability and collectively impeding the company's business materially.

Director's Statement on Selective Disclosure Regarding Cybersecurity Incidents

In a follow-up to his statement made on May 21, Erik Gerding, the director of the Division of Corporation Finance, released a statement clarifying that the SEC's recently adopted cybersecurity rules do not prohibit companies from discussing cybersecurity incidents beyond what is included in an Item 1.05 Form 8-K disclosing the incident. Recognizing that companies could have concerns that privately disclosing additional information regarding a material cybersecurity incident beyond what was included in a related Item 1.05 Form 8-K could implicate Regulation FD and require prompt public disclosure, Gerding noted that nothing in Item 1.05 alters Regulation FD or makes it apply any differently to communications regarding cybersecurity incidents. Gerding further noted that there are several ways a company can privately share information regarding a material cybersecurity incident beyond what was disclosed in its Item 1.05 Form 8-K without implicating Regulation FD requirements. For example, the information being privately shared may be immaterial or the parties with whom the company is sharing such information may not be the types of persons covered by Regulation FD that would require public disclosure, such as sharing information with a person who owes a duty of trust or confidence to a public company (*e.g.*, an attorney, investment banker, or accountant) or if the person with whom the information is being shared agrees to keep the disclosed information confidential (*e.g.*, through a Regulation FD compliant confidentiality agreement).

Conclusion

The SEC's release of additional C&DIs and Gerding's statement not only underscores the SEC's heightened focus on cybersecurity disclosures, but also highlights some of the issues and challenges companies face when encountering a cybersecurity incident in light of the new disclosure regime. Companies are strongly encouraged to consult with their counsel and advisors when facing a cybersecurity threat or incident.

---

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

RELATED INDUSTRIES + PRACTICES

- Corporate
- Privacy + Cyber