Cahill

July 15, 2024

# SEC Division of Corporation Finance Issues Additional Guidance Relating to Cybersecurity Incident Disclosure

**Recognizing the need for more clarity, Erik Gerding, Director of the Division of Corporation Finance of the Securities and Exchange Commission (the "SEC"), issued statements in May and June, providing guidance relating to the SEC's recently adopted disclosure rules about cybersecurity incidents. The new guidance clarifies that disclosure of cybersecurity incidents should only be made under Item 1.05 of Form 8-K ("Item 1.05") if the company deems the incident to be *material*. Other non-material incidents may nevertheless be disclosed under Item 8.01 of Form 8-K. The new SEC guidance also reassures issuers that Regulation FD does not prohibit the private disclosure of additional incident detail beyond what is in an Item 1.05 disclosure, noting the importance of sharing such information for remediation and mitigation efforts.**

## Background

On July 26, 2023, the SEC adopted new rules requiring public companies to disclose information relating to material cybersecurity incidents within four business days under Item 1.05. According to the new rules, a cybersecurity incident should be deemed "material" and disclosed 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."[1] Without specifying any particular details to be included, the new rules require incident disclosures under Item 1.05 to describe the material aspects of the nature, scope, and timing of the incident, along with the anticipated impact.

Although the new disclosure obligations became effective on December 18, 2023, a fair amount of uncertainty remains about how the rules operate in practice. Some issuers have made disclosures under Item 1.05 about incidents that have been explicitly described as *not* material or as to which the determination of materiality was ongoing. Others were reportedly concerned that sharing otherwise undisclosed information and details about a cybersecurity incident with vendors and others could violate Regulation FD. The new guidance recognizes that determining materiality can take time and can evolve based upon developing information and investigation. Director Gerding's May and June statements directly address these issues, and provide additional insight into the SEC's views regarding disclosure obligations under Item 1.05.

## May 2024 Guidance

On May 21, 2024, Director Gerding issued a statement titled "Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents" (the "May Guidance") providing clarifying guidance

---

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

about the applicability of Item 1.05 to incidents that have not been determined to be material or for which a determination of materiality is still ongoing. The May Guidance describes disclosure of non-material incidents as "voluntary disclosures" that Director Gerding distinguishes from statements made under Item 1.05, noting: "Item 1.05 is not a voluntary disclosure, and it is by definition material because it is not triggered until the company determines the materiality of an incident."[2] As a result, Item 1.05 is *exclusively* reserved for incidents that have been deemed material. Incidents that are still under investigation or that have been determined to not be material should not be disclosed under Item 1.05, according to the May Guidance. Instead, voluntary disclosure of other incidents is properly made under Item 8.01 (Other Events) of Form 8-K. Director Gerding also pointedly notes the following with respect to evolving determinations:

> 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, then it should file an Item 1.05 Form 8-K within four business days of such subsequent materiality determination. That Form 8-K may refer to the earlier Item 8.01 Form 8-K, but the company would need to ensure that the disclosure in the subsequent filing satisfies the requirements of Item 1.05.[3]

The May Guidance notes that a filing under Item 1.05 in the absence of or before a materiality determination is likely to confuse investors, and the "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."[4]

Director Gerding notes that the May Guidance is not intended to discourage voluntary disclosure of cybersecurity incidents that do not meet Item 1.05's disclosure threshold. In fact, the May Guidance acknowledges the importance of voluntary disclosures of non-material incidents to the marketplace and the disclosing companies. The May Guidance is intended to avoid investor confusion and prevent dilution of the value of Item 1.05, addressing the concern that "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."[5]

## June 2024 Guidance

A second clarifying statement was issued on June 20, 2024, titled "Selective Disclosure of Information Regarding Cybersecurity Incidents" (the "June Guidance"). It addresses apparent uncertainty about the applicability of Regulation FD to Item 1.05 disclosures and the scope of information that could be shared privately once a disclosure had been made under that Item. Addressing the concern that Item 1.05 disclosures regarding material incidents could effectively preclude companies from privately sharing any undisclosed details about the incident under Regulation FD, even to vendors and contract parties, Director Gerding seeks to clarify that this is not the case:

> Nothing in Item 1.05 prohibits a company from privately discussing a material cybersecurity incident with other parties or from providing information about the incident to such parties beyond what was included in an Item 1.05 Form 8-K. Those parties may include commercial counterparties, such as vendors and

---

[2] https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-incidents-05212024.

[3] *Id*.

[4] *Id*.

[5] *Id*.

customers, as well as other companies that may be impacted by, or at risk from, the same incident or threat actor.[6]

The June Guidance notes that such additional disclosures have value for "remediation, mitigation, or risk avoidance efforts" and offers various contexts and bases upon which sharing of details for a material incident can be made:

> There are several ways that a public 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. For example, the information that is being privately shared about the incident may be immaterial, or the parties with whom the information is being shared may not be one of the types of persons covered by Regulation FD. Further, even if the information being shared is material nonpublic information and the parties with whom the information is being shared are the types of persons covered by Regulation FD, an exclusion from the application of Regulation FD may apply. For example, if the information is being shared with a person who owes a duty of trust or confidence to the issuer (such as an attorney, investment banker, or accountant) or if the person with whom the information being shared expressly agrees to maintain the disclosed information in confidence (*e.g.*, if they enter into a confidentiality agreement with the issuer), then public disclosure of that privately-shared information will not be required under Regulation FD.[7]

The June Guidance highlights that SEC rules generally do not prohibit the sharing of information regarding material cybersecurity incidents, even if certain of such information is not specifically mentioned in the Item 1.05 disclosure. As for Regulation FD, Director Gerding notes that it has been in place for twenty years, and public companies should be familiar with navigating it, and "if the scope and requirements of those rules are heeded, they should not pose an undue impediment to the mutually beneficial sharing of information regarding material cybersecurity incidents."[8]

## Conclusion

The disclosure of cybersecurity incidents, both material and immaterial, continues to be a challenging and uncertain area in which the SEC rules and guidance are continually evolving and subject to additional clarification. The latest rules are leading to both over- and under-disclosure challenges, as companies undertake to provide the right mix of information called for by the rules. The new guidance is helpful in answering some of the open questions. Further statements and guidance from the SEC are likely as these issues percolate.

* * *

If you have any questions about these matters or strategies for compliance with SEC rules relating to disclosure of material and non-material cyber and other security incidents, please do not hesitate to contact authors David Owen (Partner) at 212.701.3955 or DOwen@cahill.com; or Ken Ritz (Associate) at 212.701.3661 or KRitz@cahill.com; or email publicationscommittee@cahill.com.

---

[6] https://www.sec.gov/newsroom/whats-new/gerding-cybersecurity-incidents-06202024

[7] *Id.*

[8] *Id.*