Published on *The National Law Review* https://natlawreview.com

# SEC Issues New Statement on Cybersecurity Incident Disclosure

Article By:

Daniel T. Kajunski

Anne L. Bruno

Cynthia J. Larose

Raven Sun

Last week, Erik Gerding, Director of the SEC's Division of Corporation Finance (the Division), issued a statement[1] providing clarification regarding the disclosure of cybersecurity incidents by reporting companies. This follows the cybersecurity rules adopted on July 26, 2023, which, among other things, require that material cybersecurity incidents be disclosed under Item 1.05 of Form 8-K (See our earlier Viewpoints advisory).

The SEC's clarification also follows an initial flurry of "voluntary" disclosures of cybersecurity incidents under Item 1.05 of Form 8-K by reporting companies that did not appear to have made any determination related to the materiality of the reported incidents at the time of filing the Item 1.05 Form 8-K.

**Here are the key points from Erik Gerding's statement.** For more detailed information, please refer to the full statement from Erik Gerding here.

1. ***Mandatory Disclosure Upon Materiality Determination***:

- According to the cybersecurity rules adopted on July 26, 2023, reporting companies are required to disclose material cybersecurity incidents under Item 1.05 of Form 8-K. This mandatory disclosure is triggered once the reporting company determines the incident is material. The Division's clarification emphasizes that the required filing under the cybersecurity rules is not voluntary, in response to the noted Form 8-K filings by some reporting companies that seem to have been made in an abundance of caution.

2. ***Key Takeaway: Voluntary Disclosuresof Non-Material Incidents***:

- Item 1.05 of Form 8-K does not expressly prohibit voluntary disclosure of non-material cybersecurity incidents or incidents still under materiality assessment, as the SEC recognizes that such disclosures would provide value to investors and the market.
- Voluntary disclosure of non-material incidents or incidents where materiality has not yet been determined should be made under a different item of Form 8-K (for example, Item 8.01). This would help avoid investor confusion (a major concern of the Division) and maintain the significance of Item 1.05 disclosures.

3. ***Updating Disclosures Upon Materiality Determination***:

- If a reporting company initially discloses a cybersecurity incident under Item 8.01 and later determines it is material, it is required to file an Item 1.05 Form 8-K within four business days of the determination.
- The subsequent Item 1.05 Form 8-K should refer to the earlier Item 8.01 disclosure and meet all requirements of Item 1.05 of Form 8-K; therefore, the full disclosure of incidents may require multiple SEC filings.

4. ***Materiality Assessment***:

- When assessing the materiality of a cybersecurity incident, reporting companies should take into account both qualitative and quantitative factors. These factors would include not only the impact (or reasonably likely impact) on financial condition and operational results but also potential harm to reputation, relationships with customers or vendors, competitiveness, and the likelihood of litigation or regulatory actions, including those initiated by state, federal, and non-US authorities.
- Even if the full impact (or reasonably likely impact) of the incident remains undetermined, cybersecurity incidents that are considered significant are required to be disclosed under Item 1.05 of Form 8-K, with a note that the impact assessment is ongoing. Reporting companies are also required to amend the Form 8-K to include the impact once it is known.

## Foreign Private Issuers:

Foreign private issuers filing on Form 6-K would not be impacted by this statement. Unlike Form 8-K, Form 6-K does not have an equivalent to Item 1.05. Instead, Form 6-K requires foreign private issuers to disclose material cybersecurity incidents that have been publicized in a foreign jurisdiction, to any stock exchange or to securityholders. However, there is no mandatory location specified within Form 6-K for these disclosures.

## Compliance Timeline:

- For all reporting companies, other than smaller reporting companies, compliance with Item 1.05 of Form 8-K has been required since ***December 18, 2023***.
- Smaller reporting companies are required to comply with Item 1.05 beginning ***June 15, 2024***.

## Importance for Investors and Reporting Companies:

Emphasizing the importance of distinguishing between material and non-material incidents, the new guidance on cybersecurity incident disclosure offers criteria for making such distinctions, thus

preventing investor confusion. This clarity is important for informed investment and voting decisions. Accurate classification and timely disclosure are essential in maintaining transparency and trust in the market. Reporting companies should diligently assess and disclose cybersecurity incidents by these guidelines to ensure compliance and preserve market integrity.

**Endnotes**

**[1]** Director Gerding's statement is not a rule, regulation, or statement of the SEC, and it has no legal force or effect. According to the SEC, the statement does not alter or amend applicable law, and it creates no new or additional obligations for any person.



National Law Review, Volume XIV, Number 193