WINSTON & STRAWN LLP

BLOG

SEC Issues Additional Guidance on Cybersecurity Incident Disclosure

JULY 10, 2024

NEW C&DIS

On June 24, 2024, the U.S. Securities and Exchange Commission (SEC)'s Division of Corporation Finance released five new Compliance and Disclosure Interpretations (C&DIs) covering the disclosure of cybersecurity incidents under Item 1.05 of Form 8-K. The new C&DIs (104B.05 through .09) can be found on the SEC's website. These C&DIs relate to the final rules adopted by the SEC in July 2023 that require public companies to disclose material cybersecurity incidents and enhance and standardize periodic disclosure of cybersecurity risk management, strategy, and governance. You can find our initial discussion of the final rules here.

KEY TAKEAWAY

The new C&DIs address specific scenarios involving the effect of ransomware payments on registrants' disclosure obligations and materiality assessments under Form 8-K Item 1.05. Notably, the guidance reaffirms that making a ransomware payment to remedy a cybersecurity incident does not automatically exempt a registrant from assessing the incident's materiality or fulfilling its reporting requirements under Item 1.05. The SEC also notes that registrants must evaluate the materiality of related incidents collectively, regardless of whether such related incidents were individually determined to be immaterial.

CONTINUATION OF THE SEC'S FOCUS ON CYBERSECURITY

These new C&DIs supplement four previous C&DIs issued by the SEC in December 2023 (104B.01 through .04), which discuss situations wherein a registrant requests that the U.S. Attorney General determine whether disclosure of a cybersecurity incident would pose a substantial risk to national security or public safety and such disclosure therefore should be withheld.

Recent statements on May 21, 2024 and June 20, 2024 from Erik Gerding, Director of the SEC's Division of Corporation Finance, further contextualize these guidelines.

On May 21, 2024, Director Gerding noted that the purpose of Item 1.05 of Form 8-K is to disclose incidents that registrants deem to be material and that, to avoid confusing investors and diluting the significance of material disclosures under Item 1.05, voluntary disclosures of incidents that registrants either deem immaterial or of which

they have not yet determined the materiality should be filed under Item 8.01. He also noted that if a registrant subsequently determines that a previously disclosed incident under Item 8.01 is actually material to the registrant, such incident should be disclosed within four business days of such determination under Item 1.05.

On June 20, 2024, Director Gerding addressed concerns about selective and private disclosure of cybersecurity incidents outside of a registrant's Form 8-K and the potential Regulation FD implications. Director Gerding noted that there are several ways in which a registrant can privately discuss cybersecurity incidents without triggering Regulation FD's public disclosure requirements and provided a few examples.

The release of the new C&DIs, together with the recent comments by Director Gerding, emphasize the SEC's ongoing focus on disclosure of cybersecurity incidents.

2 Min Read

Authors

David Sakowitz

Jacob Tabman

Pete Staviski

Related Topics

Capital Markets | Public Company | Securities and Exchange Commission (SEC) | Cyber Security

Related Capabilities

Capital Markets | Public Companies | Corporate Governance

Related Professionals

David Sakowitz

Jacob Tabman

Pete Staviski

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.