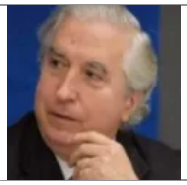

John C. Coffee, Jr. – Mass Torts and Corporate Strategies: What Will the Courts Allow?

By John C. Coffee, Jr.

Compliance's Next Challenge: Polarization

By Miriam H. Baer

Will the Common Goo Guys Come to the Shootou in SEC v. Jarkesy? And Why It Matters

By Eric W. Orts

Editor-At-Large
Reynolds Holding

THE CLS BLUE SKY BLOG

COLUMBIA LAW SCHOOL'S BLOG ON CORPORATIONS AND THE CAPITAL MARKETS

Editorial Board
John C. Coffee, Jr.
Edward F. Greene
Kathryn Judge

Skadden Discusses FBI, DOJ, and SEC Guidance on Disclosing Cybersecurity Incidents

By Brian V. Breheny, Raquel Fox, William Ridgway, David A. Simon and Khadija L. Messina January 3, 2024

Comment

The U.S. Securities and Exchange Commission (SEC) adopted final rules in 2023 that are intended to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance and incident reporting by public companies (including foreign private issuers). The SEC Form 8-K Item 1.05 cybersecurity incident reporting rules, which became effective on December 18, 2023, provide that companies may delay the required disclosure (which becomes public immediately upon filing) if it poses a substantial risk to national security or public safety. Last week, the Federal Bureau of Investigation (FBI), the U.S. Department of Justice (DOJ) and the SEC each released guidance on how companies may request this exception and how determinations will be made.

Form 8-K Cybersecurity Incident Reporting

Item 1.05 of Form 8-K requires disclosure within four business days after a company determines that a "cybersecurity incident" experienced by the company is material. An instruction to Form 8-K provides that materiality determinations must be made "without unreasonable delay" after discovery of a cybersecurity incident, and the SEC states in the adopting release that "adhering to normal internal practices and disclosure controls and procedures will suffice to demonstrate good faith compliance."

However, the final rules provide that a company may delay disclosure of a material cybersecurity incident on Form 8-K:

(i) For up to 30 days if the U.S. Attorney General determines that public disclosure poses a substantial risk to national security or public safety.

(ii) For an additional period of up to 30 days if the Attorney General determines that public disclosure continues to pose a substantial risk.

(iii) For a final additional period of up to 60 days in extraordinary circumstances due to national security risks.

FBI Guidance on Requesting a Delay

On December 6, 2023, the FBI issued a policy notice describing the process for requesting a delay in public reporting of a cybersecurity incident under the SEC rule. Importantly, the notice states that companies must (i) make such requests to the FBI "concurrently" with the company's materiality decision; and (ii) provide the date and time (including time zone) of the company's materiality determination for the FBI to confirm that the request is made "immediately upon determination."

To request a delay, companies must contact the FBI through a dedicated email address: cyber_sec_disclosure_delay_referrals@fbi.gov. The FBI published guidance that outlines the information companies must include in a delay request. The request must include, among other information:

- Details of the incident (*g*., type, suspected intrusion vectors, affected data or infrastructure, known operational impacts).
- Information about the cyber actors, if known.
- The status of mitigation or remediation efforts.

DOJ Guidance on Delay Determination

On December 12, 2023, the DOJ issued guidelines on determinations for delayed public reporting of material cybersecurity incidents (DOJ Guidelines) clarifying that such determinations hinge on whether the public disclosure of a cybersecurity incident threatens public safety or national security, and not whether the incident itself poses a substantial risk to public safety and national security.

The DOJ Guidelines provide that, typically, companies will be able to publicly disclose the required material information at a level of generality that does not pose a substantial risk to national security or public safety. Therefore the DOJ expects that it will find a substantial risk to national security or public safety in only limited circumstances, which may include the following situations:

- The cybersecurity incident occurred because the illicit cyber activities are reasonably suspected to have involved a technique for which there is not yet well-known mitigation.
- The cybersecurity incident primarily impacts a system operated or maintained by a company that contains sensitive U.S. government information, or information the U.S. government would consider sensitive.
- The company's remediation efforts for any critical infrastructure or critical system remain ongoing and the disclosure required by Item 1.05(a) would undermine those remediation efforts.
- A U.S. government agency believes that public disclosure poses a substantial risk to national security or public safety.

The Attorney General must invoke the provision under SEC rules that permits delayed disclosure within four business days of a company making the determination that a cyber incident is material. Therefore, if a company believes its circumstances are likely to meet the requirements for delayed disclosure under the DOJ Guidelines, the company should provide the relevant information to the FBI as soon as possible, even if that means providing such information before the company has completed its materiality analysis or its investigation.

SEC Compliance & Disclosure Interpretations

On December 14, 2023, the SEC staff published four Compliance and Disclosure Interpretations (CDIs) regarding the national security and public safety exception and related FBI and DOJ guidance. The CDIs provide the following:

- A company that requests a delay and is awaiting a decision from the Attorney General is still required to file the Form 8-K Item 1.05 within four business days of its determination that the incident is material.
- A company must file the Form 8-K Item 1.05 within four business days of the expiration of the delay period provided by the Attorney General, even if the company's request for additional delay remains pending.
- If the Attorney General grants a delay to the company but subsequently determines and notifies the company and the SEC that disclosure of the incident no longer poses a substantial risk to national security or public safety, the company has four business days from such notification to file the Form 8-K Item 1.05.
- The fact that a company consults the DOJ regarding the applicability of delayed disclosure under Item 1.05(c) does not necessarily result in the determination that the cyber incident is material and subject to disclosure under Item 1.05(a).

Takeaways

Companies are encouraged to consult law enforcement and the relevant U.S. government agencies early in the assessment process of cybersecurity incidents where disclosure may pose a substantial risk to national security or public safety. Companies may take comfort that the SEC does not view such consultation as necessarily resulting in a determination that the cybersecurity incident is material. The DOJ expects the availability of delayed Form 8-K Item 1.05 disclosure for a material cybersecurity incident to be limited.

This post comes to us from Skadden, Arps, Slate, Meagher & Flom LLP. It is based on the firm's memorandum, "FBI, DOJ and SEC Publish Guidance on Requesting Delayed Reporting of Material Cyber Incidents on Form 8-K: Takeaways for CISOs and Disclosure Committees," dated December 19, 2023, and available here.