GT GreenbergTraurig

Alert | Data Privacy & Cybersecurity

May 2024

SEC Clarifies Confusion Concerning Cybersecurity Incident Reporting

On May 21, 2024, U.S. Securities and Exchange Commission Director of the Division of Corporation Finance Erik Gerding issued a statement clarifying when the SEC expects companies to disclose a cyber incident. This clarification helps guide public companies who wish to disclose a cyber incident but who have not yet determined if the incident is material to file under Item 8.01 for voluntary disclosures, instead of Item 1.05, which applies only to material cybersecurity incidents.

Recap of the SEC Rule Disclosure Requirements

To summarize, the SEC Rule and the obligations thereunder require the following:

1. That if a publicly traded company determines that a cybersecurity incident is material, it must disclose a description of the material aspects of the nature, scope, and timing of the incident *within **four** business days of the determination that the incident is material*.

2. This disclosure must be made by filing a Form 8-K in accordance with the rules governing the Securities Exchange Act of 1934.

3. A materiality determination must be made without unreasonable delay after the discovery of an incident.

4. The only basis for delaying the four-business-day timeline for submitting a report is a direct request from the U.S. Attorney General, in writing, to protect national security or public safety.

5. The Form 8-K should address the following points, to the extent known:

    a) A general description of when the incident was discovered and whether it is ongoing;

    b) A brief description of the nature and scope of the incident;

    c) Whether any data was stolen or altered in connection with the incident;

    d) The effect or reasonably likely effect of the incident on the company's operations, including its financial condition or results of operations; and

    e) Whether the company has remediated or is currently remediating the incident.

Over Reporting Under Item 1.05

As GT previously reported, since the SEC's Cybersecurity Incident Disclosure Rule (SEC Rule) took effect on Dec. 18, 2023, about a dozen companies have filed a Form 8-K reporting a material cybersecurity incident. GT noted five noticeable trends, including reporting by companies who had not yet confirmed material impact on financial condition or results of operations, and reporting by companies who later determined there was no material impact from the cybersecurity incident. Review of these early Item 1.05 filings reflects confusion in the marketplace over when materiality is triggered for reporting purposes and concern among some public companies that they will be faulted for not making a timely report.

The SEC took notice of these trends. In the statement, Mr. Gerding notes that the SEC did not wish to "discourage companies from voluntarily disclosing cybersecurity incidents for which they have not yet made a materiality determination, or from disclosing incidents that companies determine to be immaterial," because such disclosures could have value to investors, the marketplace, and companies. However, the SEC is clear that Item 1.05 is specifically for incidents the registrant deems material, stating that its use for immaterial or undetermined incidents could confuse investors.

The SEC instead directs companies who wish to disclose a cybersecurity incident that may be significant, but has not yet been deemed material, to disclose the incident under Item 8.01 Form 8-K, which applies to voluntary disclosures. Mr. Gerding opines that clear distinction between filings under Item 1.05 (material incidents) and Item 8.01 (voluntary disclosures) helps investors make informed decisions.

If an incident initially disclosed under Item 8.01 is later found to be material, a company must file an Item 1.05 Form 8-K within four business days of the determination. Per the SEC, this approach aims to provide transparency while avoiding investor confusion and preserving the integrity of disclosures regarding material cybersecurity incidents.

Companies who have incorporated the new SEC disclosure rules into their incident response plans should consider incorporating the SEC's guidance. The clarification should provide some relief to companies who fall victim to a cybersecurity incident where the materiality threshold has not been met, but who are concerned about being penalized for not timely filing a disclosure under the new cybersecurity reporting rules.

GT GreenbergTraurig

Authors

This GT Alert was prepared by:

- Jena M. Valdetero | +1 312.456.1025 | Jena.Valdetero@gtlaw.com
- Steven M. Malina | +1 312.476.5133 | Steven.Malina@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Berlin.¬ Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Houston. Kingdom of Saudi Arabia.« Las Vegas. London.* Long Island. Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Diego. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Singapore.⁻ Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ United Arab Emirates.‹ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.