

## 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.

## Authors

This GT Alert was prepared by:

- [Jena M. Valdetero](#) | +1 312.456.1025 | [Jena.Valdetero@gtlaw.com](mailto:Jena.Valdetero@gtlaw.com)
- [Steven M. Malina](#) | +1 312.476.5133 | [Steven.Malina@gtlaw.com](mailto:Steven.Malina@gtlaw.com)

Albany. Amsterdam. Atlanta. Austin. Berlin.<sup>7</sup> Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Houston. Kingdom of Saudi Arabia.<sup>6</sup> Las Vegas. London.<sup>8</sup> Long Island. Los Angeles. Mexico City.<sup>5</sup> Miami. Milan.<sup>9</sup> Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Diego. San Francisco. Seoul.<sup>10</sup> Shanghai. Silicon Valley. Singapore.<sup>11</sup> Tallahassee. Tampa. Tel Aviv.<sup>12</sup> Tokyo.<sup>13</sup> United Arab Emirates.<sup>14</sup> Warsaw.<sup>15</sup> Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. <sup>7</sup>Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. <sup>8</sup>Operates as a separate UK registered legal entity. <sup>6</sup>Greenberg Traurig operates in the Kingdom of Saudi Arabia through Greenberg Traurig Khalid Al-Thebity Law Firm, a professional limited liability company, licensed to practice law by the Ministry of Justice. <sup>5</sup>Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. <sup>9</sup>Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. <sup>10</sup>Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. <sup>11</sup>Greenberg Traurig's Singapore office is operated by Greenberg Traurig Singapore LLP which is licensed as a foreign law practice in Singapore. <sup>12</sup>Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. <sup>13</sup>Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. <sup>14</sup>Greenberg Traurig's United Arab Emirates office is operated by Greenberg Traurig Limited. <sup>15</sup>Greenberg Traurig's Warsaw office is operated by GREENBERG TRAUIG Nowakowska-Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAUIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2024 Greenberg Traurig, LLP. All rights reserved.*