GT GreenbergTraurig

# Alert | Data Privacy & Cybersecurity

April 2024

## 5 Trends Under SEC's New Cybersecurity Incident Disclosure Rule

Since the Securities and Exchange Commission's Cybersecurity Incident Disclosure Rule (SEC Rule) took effect Dec. 18, 2023, about a dozen companies have filed a Form 8-K reporting a material cybersecurity incident. This GT Alert discusses the trends on how companies have made these disclosures thus far. In short, the companies who have filed an 8-K have erred on the side of caution, hedging on whether the materiality threshold has been met, reporting an incident early, and providing only high-level information about the incident.

### Recap of the SEC Rule Disclosure Requirements

GT wrote a series of alerts and blogs on the SEC Rule and the obligations thereunder.[1] As a recap, the SEC Rule requires the following:

- 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*.

[1] *See* in chronological order: GT Alert from March 24, 2022 (Discussing the SEC Rule's proposal); GT Alert from July 31, 2023 (Discussing the finalize SEC Rule); GT blog post from Jan. 3, 2024 (Discussing the DOJ Guidelines on the National Security Exception for Disclosure).

- This disclosure must be made by filing a Form 8-K in accordance with the rules governing the Securities Exchange Act of 1934.
- A materiality determination must be made without unreasonable delay after the discovery of an incident.
- 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.[2]
- The Form 8-K should address the following points, to the extent known:
  - A general description of when the incident was discovered and whether it is ongoing;
  - A brief description of the nature and scope of the incident;
  - Whether any data was stolen or altered in connection with the incident;
  - The effect or reasonably likely effect of the incident on the company's operations, including its financial condition or results of operations; and
  - Whether the company has remediated or is currently remediating the incident.

## Trends

Looking at the disclosures companies have made up until today, there are five noticeable trends:

1. **Reporting companies are disclosing even if they later determine there was no material impact from the cybersecurity incident.** Companies are disclosing cybersecurity incidents even when they later report in an updated filing that the incident did not ultimately have a material impact on the company's operations or financial condition. Therefore, the current trend as to the materiality determination for reporting companies appears to be, "when in doubt, disclose."

2. **Initial disclosures are brief and generic.** The initial disclosures on the cybersecurity incident are generally short and general. Companies are not providing exact numbers of impacted individuals or monetary loss, and the operations or systems impacted are only vaguely described.

3. **Many of the initial filings read like high-level press releases.** Companies typically are sticking to a script stating they have taken actions to contain, assess, and remediate the incident, they have engaged external cybersecurity and/or legal experts, they are still investigating, and they are cooperating with law enforcement. Where personally identifiable information (PII) is involved, companies generally state that relevant regulators and affected persons will be notified, as required by applicable data protection or breach notification laws.

4. **Reporting companies have not yet confirmed material impact on financial condition or results of operations.** As of this writing, GT identified no company who has reported that an incident was reasonably likely to materially impact its financial condition or results of operations. Note that a few companies have indicated in their initial filing that they are still investigating the impact.

[2] DOJ Material Cybersecurity Incident Delay Determinations, Dec. 12, 2023.

5. **Updated disclosures.** As of this writing, just under half of the companies that have filed 8-K cybersecurity disclosures have updated their initial filings. The updated disclosures typically contain slightly more information than the initial filing and an update on whether the investigation is closed or if business operations have been resumed.

## Authors

This GT Alert was prepared by:


- Jena M. Valdetero | +1 312.456.1025 | Jena.Valdetero@gtlaw.com
- Wouter van Wengen | +31 20 301 7445 | Wouter.vanWengen@gtlaw.com