Privacy Alert
May 2024

SEC Director Sheds Light on Cybersecurity Reporting Obligations

Since the Securities and Exchange Commission (SEC) amended Form 8-K in late 2023 to include Item 1.05, requiring public companies to disclose any cybersecurity incident a company determines to be material, chief privacy officers and chief information security officers have grappled with determining which incidents qualify as material for SEC reporting purposes. In general, materiality has long been viewed from the perspective of a reasonable investor and whether the information at issue (i.e., cybersecurity incident) has a substantial likelihood of significantly altering the "total mix" of information made available in connection with an investment decision.

Now we have guidance on this topic. On May 21, the director of the SEC's Division of Corporation Finance issued a statement addressing Disclosure of Cybersecurity Incidents Determined to be Material and Other Cybersecurity Incidents. In it, Director Gerding addressed the recent requirement that public companies must disclose material cybersecurity incidents under Item 1.05 of Form 8-K, and what he views as some companies' "confusing" use of Item 1.05 to disclose immaterial or not-yet-material information.

Material versus non-material incidents. If a cybersecurity event is **material**, a company must take the following steps:

- Disclose the nature, scope and timing of the incident.
- Disclose the material impact, or reasonably likely material impact, of the incident.
- Complete Item 1.05 of Form 8-K within **four** business days of the date the event was deemed material.

If immediate disclosure would pose a substantial risk to national security or public safety, a process exists for requesting a delay in reporting.

For **non-material events**, or incidents for which a materiality determination has not yet been made, Director Gerding recommended that a company should address those under Item 8.01 of Form 8-K. To be clear, Director Gerding indicated that the clarification was not intended to discourage companies from voluntarily disclosing immaterial cybersecurity incidents or incidents for which they have not yet made a materiality determination.

Instead, the director wanted to ensure that investors were not confused about the materiality of any disclosure under Item 1.05. He noted that, in adopting Item 1.05, the SEC stated that "[i]tem 1.05 is not a voluntary disclosure, and it is by definition material because it is not triggered until the company determines the materiality of an incident." If a company makes a voluntary disclosure under Item 8.01 and later determines that the incident is material,

Attorney Advertising

then that company must file an Item 1.05 Form 8-K within four business days of the subsequent materiality determination. In addition, Director Gerding noted that if the impact of a material incident was not yet determined, an amendment to the Item 1.05 Form 8-K should be filed to disclose the impact once that information became available.

Finally, Director Gerding noted that the assessment of potential impact on the company should not be limited to its financial condition and results of operation. Instead, the determination should also include qualitative factors. For example, companies should consider whether the incident would harm its reputation, relationships or competitiveness, or potentially result in litigation or regulatory investigations or actions.

Key Takeaways. As a follow up to this published statement, publicly traded companies should take the following steps:

- Train key personnel (and the board) to identify and address cybersecurity incidents, and ensure that they have access to members of management who participate in making disclosure determinations.
- Follow clear, consistent and reliable practices for rigorous and fulsome materiality assessments of cybersecurity incidents, which should involve appropriate subject matter experts and legal specialists.
- Document materiality assessment processes with guidance from counsel.
- Ensure timely and complete disclosure under Item 1.05 when a cybersecurity incident is deemed material; if the company has not yet determined that an incident is material, carefully evaluate the risks and opportunities of disclosure under Item 8.01.

To read the full statement, click here to visit the SEC's website. Director Gerding's statement, while made in his official agency capacity, is, itself, not a rule, regulation or statement of the SEC.

Related Professionals

Giovanni Caruso . . . . . gcaruso@loeb.com
Harry Valetk . . . . . hvaletk@loeb.com