BCLP. Client Intelligent

BCLPSecCorpGov.com

SEC STAFF PUBLISHES NEW GUIDANCE FOR HANDLING CYBERSECURITY INCIDENTS

Jun 24, 2024

WHAT HAPPENED

On June 24, 2024, the SEC's Division of Corporation Finance published five additional interpretations (CDIs) addressing the effect of ransomware payments on the obligation of companies to report material cybersecurity incidents in Item 1.05 8-K filings. These supplement four previous CDIs addressing the effect of consultation with or national security findings by Attorney General.

The new CDIs follow on the heels of:

- The CorpFin Director's recent statement regarding selective disclosure and the ability of companies to rely on traditional Regulation FD practices to share information about material incidents with commercial partners.
- The SEC staff's guidance for use of Item 1.05 of Form 8-K versus Item 8.01 of Form 8-K, as discussed in our May 29, 2024 post.

TAKEAWAYS

As discussed in our July 27, 2023 post, the SEC's new Item 1.05 8-K rule took effect late last year for most companies, or this month for smaller reporting companies.

Companies should consult the new guidance whenever evaluating the materiality of cybersecurity incidents and their potential 8-K reporting obligations.

DEEPER DIVE

Effect of ransomware payments. The new staff guidance address five scenarios involving ransomware payments, generally concluding that such payments do not relieve companies of their obligations to evaluate materiality or make Item 1.05 8-K filings:

- *If paid before determining materiality, company must still evaluate 8-K obligation.* The cessation of an incident before any materiality determination, including as a result of making a ransomware payment, does not relieve the company of the requirement to make a materiality determination.

- *If incident is material, the company must still file Item 1.05 8-K.* If the company determines an incident is material, then a subsequent ransomware payment and cessation of the incident does not relieve the company of the requirement to file an Item 1.05 8-K.

- *Ransomware insurance coverage does not necessarily prevent materiality determination.* The availability of insurance to reimburse for ransomware payments does not obviate the need to consider other relevant factors in evaluating materiality.

- *The small size of a ransomware payment does not necessarily make the incident immaterial.* The SEC views a ransomware payment as only one of many factors that companies need to consider in evaluating materiality.

- *Materiality of multiple ransomware payments for individual immaterial incidents.* A company that experiences multiple incidents involving ransomware attacks should consider whether any incidents were related and, if so, whether they are collectively material.

Effect of AG consultation. These interpretations supplement the four CDIs the staff published last December regarding the effect of consultation with or national security findings by Attorney General:

- *Merely requesting delay from AG does not change filing deadline.* Requesting a delay does not change the filing deadline. An 8-K delay is available only if (1) the Attorney General determines that disclosure would pose a substantial risk to national security or public safety and (2) the AG notifies the SEC in writing before the 8-K due date.

- *8-K required at expiration of delay unless AG grants additional relief.* If the AG declines to approve an additional delay before expiration of the current delay period, the company must file an Item 1.05 8-K within four business days of the expiration date.

- *8-K triggered if AG changes decision.* If the AG initially approves a delay but later changes his or her mind, then the company must file an Item 1.05 8-K within four business days of the AG's notification to the SEC.

- *Discussion with DOJ does not itself trigger materiality.* Consultation with DOJ or other government agency does not by itself necessitate a determination of materiality.

Selective disclosure of incidents. The Director's statement reminds companies that they can share information about material incidents with commercial partners, such as vendors and customers, or

other companies affected by the same risk or threat, using conventional Regulation FD methods. Under FD, sharing is permissible if:

- The incident is immaterial.
- The recipient is not a covered person, such as a market professional or security holder.
- The recipient owes a duty of trust or confidence with the company, such as an attorney, investment banker or accountant.
- The recipient agrees to keep the information confidential.

The Director expressed concern that "some companies are under the impression that if they experience a material cybersecurity incident, the Commission's new rules prohibit them from discussing that incident beyond what was included in the Item 1.05 Form 8-K disclosing the incident. That is not the case."

RELATED CAPABILITIES

- Securities & Corporate Governance

MEET THE TEAM

R. Randall Wang

St. Louis

randy.wang@bclplaw.com
+1 314 259 2149

professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.