Blogs
December 18, 2023
Corp Fin (and the DOJ and FBI) Issue Cybersecurity “Limited Disclosure Exception” Guidance

We got some guidance from Corp Fin, the Department of Justice and the FBI last week related to the SEC's new cybersecurity disclosure rules adopted back in July (this blog covers what those rules require).

In the new rules, there is a narrow, time-limited exception to the Item 1.05 Form 8-K disclosure requirement for material cybersecurity incidents if the US Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing. This new guidance explains the process and parameters of this limited exception.

Corp Fin's Guidance

Corp Fin issued four CDIs regarding new Item 1.05 of Form 8-K, which are summarized below. In addition, Corp Fin Director Erik Gerding provided an informative speech on the cybersecurity disclosure rules, with insight on how the rules evolved from the proposed to final formulations and what is – and is not – required.

1. Question 104B.01: If a company experiences a material cybersecurity incident and asks the Attorney General for a determination of whether disclosure of the incident on Form 8-K poses a substantial risk, but the Attorney General declines to make that determination or doesn't respond before the Form 8-K would otherwise be due, the company must still file the Form 8-K within four business days of its determination that the incident was material.

2. Question 104B.02: If a company asks the Attorney General for a determination that Form 8-K disclosure of a material cybersecurity incident poses a substantial risk and the Attorney General agrees with the company that disclosure would pose a substantial risk to national security or public safety – and also notifies the SEC that disclosure should be delayed for the time period provided in Form 8-K Item 1.05(c) – the company must file the Form 8-K within four business days of the delay period expiration given by the Attorney General.

If the company then requests an additional delay, but the Attorney General rejects or does not timely respond to the request before the expiration of the existing delay period, the Form 8-K deadline is still four business days after the expiration of the existing delay period.

3. Question 104B.03: If disclosure on Form 8-K is delayed for up to 30 days, as permitted by the Attorney General, but the Attorney General then determines, during the delay period, that disclosure no longer poses a substantial risk to national security or public safety and notifies the SEC and the company of this new determination, the company must file the Form 8-K within four business days of the Attorney General's notification to the SEC and the company.

4. Question 104B.04: Companies may consult with the DOJ or any other law enforcement or national security agency about a material cybersecurity incident, but mere consulting about a possible disclosure delay is not a determination that the incident itself is material and therefore reportable under the requirements of Item 1.05(a). Rather, the determination of whether an incident is material "is based on all relevant facts and circumstances surrounding the incident, including both quantitative and qualitative factors, and should focus on the traditional notion of materiality as articulated by the Supreme Court."

DOJ's Guidance

At the same time that Corp Fin issued these CDIs, the DOJ issued this guidance – "Department of Justice Material Cybersecurity Incident Delay Determinations" – for companies to follow if they seek permission from the DOJ to authorize a delay in reporting a cyber incident on Form 8-K.The DOJ's guidance makes clear that the key inquiry is whether ***public disclosure*** of a cybersecurity incident threatens public safety or national security – not whether the ***incident itself*** poses a substantial risk.

The DOJ believes that most companies will make disclosure of the information required by Form 8-K "at a level of generality that does not pose a substantial risk to national security or public safety," and thus the DOJ won't typically grant permission to delay disclosure. But the DOJ's guidance does list four categories of circumstances – at least, initially – that might lead the DOJ to grant permission:

1. The cyber incident involved technique for which there is not yet any well-known mitigation and the public disclosure could lead to more cyber incidents;

2. The cyber incident involves system operated or maintained by a company that contains sensitive US government information or information that the government would consider sensitive and public disclosure could make that information and/or system vulnerable;

3. The company is engaged in remediation efforts for a critical infrastructure or system and public disclosure revealing that the company is aware of the incident would undermine those remediation efforts; or

4. A government agency makes a company aware of a cybersecurity incident for which the agency believes delayed disclosure is appropriate, the company agrees with this position, and the agency seeks permission from the DOJ for a delay.

FBI's Guidance

A few days before Corp Fin and the DOJ issued guidance, the FBI issued this guidance on the process to request a disclosure delay related to cyber incidents that could pose a substantial risk to national security or public safety. The requisite process includes written notice directly to the FBI at a soon-to-be-established dedicated email address, or through the Secret Service, the Department of Defense, the Cybersecurity and Infrastructure

Security Agency or another sector risk management agency. The notice must address these 10 questions:

1. What is the name of your company?
2. When did the cyber incident occur?
3. When did you make a determination to disclose a cyber incident via Form 8-K? Include the date, time, and time zone.?(Note: Failure to report this information immediately upon determination will cause your delay-referral request to be denied.)
4. Are you already in contact with the FBI or another U.S. government agency regarding this incident? If so, provide the names and field offices of the FBI points of contact or information regarding the U.S. government agency with whom you're in contact.
5. Describe the incident in detail. Include the following details, at minimum:
   - What type of incident occurred?
   - What are the known or suspected intrusion vectors, including any identified vulnerabilities if known?
   - What infrastructure or data were affected (if any) and how were they affected?
   - What is the operational impact on the company, if known?
6. Is there confirmed or suspected attribution of the cyber actors responsible?
7. What is the current status of any remediation or mitigation efforts?
8. Where did the incident occur? Provide the street address, city, and state where the incident occurred.
9. Who are your company's points of contact for this matter? Provide the name, phone number, and email address of personnel you want the FBI to contact to discuss this request.
10. Has your company previously submitted a delay referral request or is this the first time? If you have previously submitted a delay request, please include details about when DOJ made its last delay determination(s), on what grounds, and for how long it granted the delay (if applicable).

At the same time, the FBI issued this guidance to companies about how to establish a relationship with the local field offices of the FBI.

Explore more in

Corporate Law

Topics

Quick Alerts