Securities Regulation Daily Wrap Up, PUBLIC COMPANY REPORTING AND DISCLOSURE—SEC adopts material cyber incident disclosure rule, (Jul. 26, 2023)

Securities Regulation Daily Wrap Up

Click to open document in a browser

By Jay Fishman, J.D.

Under the new rule, companies must disclose a cyber breach within four days of determining the incident is material.

A July 26, 2023, open meeting resulted in the SEC adopting material cyber incident disclosure rules by a 3-2 vote, with Chair Gensler and Commissioners Crenshaw and Lizárraga approving and Commissioners Peirce and Uyeda dissenting. Erik Gerding, the Director of the Commission's Division of Corporate Finance, introduced the rules, summarized their provisions, and answered the dissenting commissioners' questions (*Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release No. 33-11216, July 26, 2023).

The approved rule summarized. In March 2022, the Commission proposed new rules, rule amendments, and form amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and material cybersecurity incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. The proposal followed from interpretive guidance issued by Commission staff in 2011 and by the Commission in 2018 on the application of existing disclosure requirements to cybersecurity risk and incidents.

New Form 8-K Item 1.05 will require registrants to disclose any cybersecurity incident they determine to be material and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the registrant, including its financial condition and results of operations. The SEC adopted final rules requiring disclosure of material cybersecurity incidents on Form 8-K and periodic disclosure of a registrant's cybersecurity risk management, strategy, and governance in annual reports. Registrants must determine the materiality of an incident without unreasonable delay following discovery and, if the incident is determined material, file an Item 1.05 Form 8-K generally within four business days of that determination.

But the disclosures may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of that determination in writing. If the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through possible exemptive orders.

Effectiveness. The final rules take effect 30 days following publication of the adopting release in the *Federal Register*. For Regulation S-K Item 106 and the comparable requirements in Form 20-F, all registrants must provide disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. With respect to compliance with the incident disclosure requirements in Form 8-K Item 1.05 and in Form 6-K, all registrants other than smaller reporting companies must begin complying on the later of 90 days after the date of publication in the *Federal Register* or December 18, 2023. Smaller reporting companies will have an additional 180 days and must begin complying with Form 8-K Item 1.05 on the later of 270 days from the effective date of the rules or June 15, 2024. Regarding compliance with the structured data requirements, all registrants must tag disclosures required under the final rules in Inline XBRL beginning one year after initial compliance with the related disclosure requirement.

Approvals. *Chair Gensler.* Chair Gensler's support for the rules arises from the escalating number of material cybersecurity breaches in the past few years, and the tremendous number of Exchange Act-reporting public

companies that have already set forth cybersecurity policies and procedures in the wake of attacks on them. He went on to say that the current state of inconsistent reporting now mandates uniform, comparable rules that ease compliance for all registrants, however large or small. Gensler believes the rules strike the right balance between under- and over-disclosure.

Commissioner Crenshaw. Commissioner Crenshaw agreed with Chair Gensler that a consistent set of disclosure requirements is needed but also remarked on the incredible costs to a company from a cyber security breach, not only to its revenue but from the lost customers and investors who withdraw from the company for fear their personal data has been compromised and the loss of reputation from which the company will never recover.

Commissioner Lizárraga. Commissioner Lizárraga came to support the rules from a belief that providing consistent disclosures following a material cyberattack would actually incentivize customers and investor to not pull out of the company. He also put faith in Director Gerding's statement that the disclosures, by being solely risk management and strategy related and not involving the technical details of the breach, would be of no use to the attackers.

Dissent. *Commissioner Peirce.* Commissioner Peirce faulted the rule for:

- Overreaching: She found the rules too granular, requiring such specific disclosures on Form 8-K that may have exceeded the Commission's authority. But Peirce was even more concerned that the level of disclosures on 8-K could give cyber criminals a roadmap for how to even more intensely corrupt a company's information systems. Director Gerding, however, responded that only a company's risk management strategy and the manager's expertise is disclosed, not the technical details of the breach, which is the only disclosure-type that would be useful to cyber criminals.
- Deadline for reporting: Peirce found the four-day deadline for reporting a cyber incident on Form 8-K to be too short, failing to give a registrant company nearly enough time to contemplate the incident after it occurred to know exactly how to describe it on Form 8-K. And she's concerned that the information provided in those four short days may be so hastily written as to inadvertently misinform investors about the incident. But Director Gerding responded that: (a) first, the rules do not say to start a report at the time an incident occurs but rather requires disclosures only after the registrant discovers and reasonably deems a cyber incident to be a "material" incident; (b) just after the registrant determines a material incident has occurred, the U.S. Department of Justice and various other government agencies are in constant communication with the registrant about how to proceed within the four day period; and (c) the registrant may attach an addendum to the 8-K disclosure alerting investors that not all the pertinent information about the incident is in this newly released 8-K but will be forthcoming.
- Effect on small business: Lastly, Peirce is concerned the cost of providing disclosures will be too big a burden for small businesses. Director Gerding responded that following rule effectiveness, small businesses will have an additional extended time to comply and may be granted further extensions or exemptions if the breached information is considered a national security event.

Commissioner Uyeda. Commissioner Uyeda's main arguments against the rules are:

1. They create a special category for only cybersecurity risks and not for any other risk-types that could be even more important to investors than cyber risks. The national security exemption too only applies to cyber risk but not to other types of risks; and
2. The rules requiring periodic disclosures after a material incident are forward-looking in nature and, therefore, require registrants to predict what is going to happen, rendering the data provided to customers and investors somewhat unreliable.

This is Release No. 33-11216.

MainStory: TopStory CyberPrivacyFeed DataBreach GCNNews PublicCompanyReportingDisclosure RiskManagement SECNewsSpeeches