Grant Thornton

# Executive Forum 2024: Financial Reporting Update

## Teaser Video Transcript

### Cybersecurity Incident Disclosures

Well, now let's get back to a discussion of the SEC cybersecurity rule as there's been some recent clarifications about its application. So to start us off, Kendra, can you remind us the content of this rule?

Sure. The SEC rule requires two types of disclosure, the annual disclosure around policies and risk management and current reporting about material incidents when it occurs. The annual disclosures in an entity's Form 10K, including information about how the entity assesses, identifies, and manages material risks from cyber security threats and whether those risks, including previous cyber security incidents have materially affected its business strategy, results of operations or financial condition.

And also to make disclosures around overall governance in this area, the current reporting for a material cybersecurity incident takes place on a Form 8K and that's due within four business days of when the entity determines that the incident is material. So the rule added item 1.05, which is aptly titled Material Cybersecurity Incidents and disclosures in this item include details about the nature, scope, and potential impact of the incident on the company's financial condition and operations. If new information arises after the filing of that initial Form 8K, companies must amend their initial filing to update those disclosures.

All right, so what interpretive guidance did the SEC provide related to this rule? CorpFin staff issued 2 statements to address questions and clarify the requirements for these cybersecurity disclosures. The first was to address voluntary disclosure of a cybersecurity incident that the company has either not yet determined to be material or that they have definitively determined is not material. The FCC staff does encourage that voluntary disclosure in a Form 8K for non-material incidents, but it notes that the new item 1.05, should be reserved only for material cybersecurity incidents.

And it's logical, right? Because that's what the section of the report is called. The staff noted that a cyber security incident that the company either hasn't determined to be material or has definitively determined to be not material could instead be reported on another section of the 8K, such as an item 8.01. And again, the SEC staff in no way intends to discourage that voluntary disclosure, but it's seeking to encourage the disclosure in a manner that that won't confuse investors or dilute the value of the material. Cybersecurity incident disclosures under item 1.05. CorpFin's director also issued a statement clarifying that companies can privately discuss material cybersecurity incidents with certain parties without triggering Regulation fair disclosure requirements.

So that means that they can share information beyond what is publicly disclosed in a Form 8K about a cybersecurity incident, as long as they're complying with Reg FD guidelines regarding who they can disclose that information to and the nature of the information that they're sharing. The staff clarified that nothing in item 1.05 alters Regulation FD or changes how it applies to communications regarding cybersecurity incidents. And finally, court and staff added a cyber security related Q&A to its Exchange Act Form 8K CNDIS to clarify certain reporting requirements for a material cyber security incident, including factors that a company might consider when it's making its materiality determination and the timing of that determination.