Lowenstein Sandler's Cybersecurity Awareness Series

Session 11 – An Update on the SEC Cyber Rules: Confusion and More Questions Than Answers

By Kathleen A. McGee and Ken Fishkin
MARCH 2024

Ken Fishkin: Hello and welcome to **Lowenstein Sandler's Cybersecurity Awareness series**. Today, I'm with Kathleen McGee, a partner at Lowenstein Sandler, and we're going to be talking about our initial assessment on the latest SEC 8-K and 10-K filings. My first question to you, Kathleen, is now that the SEC's cybersecurity rules have been in effect since December, how have companies has been reporting their breach disclosures?

Kathleen A. McGee: Well, there have been a handful of filings via 8-K submissions since December of 2023, and we've been watching those carefully—along with everybody else on the internet, who's paying attention to these sorts of things. They have said a lot, in fact, by saying very little about whether or not the incidents that occurred were material, and that's really what we're here to talk about today.

Ken Fishkin: Great, Kathleen. If a breach is considered material, does it need to be considered material from a qualitative or a quantitative perspective?

Kathleen A. McGee: Well, that is one of the debates spinning around the internet. Just to set the table a little bit, what the SEC has said for companies now in the reporting, is that once they discover an incident is material, to report the incident within four days. The question then becomes: what constitutes a material event? And "material" has been defined by the SEC incredibly broadly—they're saying that "material" is whether or not an incident is reasonably likely to materially impact a company's financial condition or the results of their operations. And that makes it really difficult for a company to decide how and when they should actually report.

What we have seen so far in the 8-K filings are reports that are really, you know, qualitative; they're forward looking, and they're discussing in very general terms that they don't expect the series of events to impact their future operations. They are also notably saying that these events weren't material. There is no discussion—or very little discussion—about the, you know, quantity, the quantitative impact that the cyber event might have had on a company.

Ken Fishkin: Is a material breach related to just disclosing sensitive information?

Kathleen A. McGee: Absolutely not, and that's been one of the biggest impacts of these new mandated disclosures. Traditionally, for companies and entities—whether they were for profit or not—the issue was someone's PII or sensitive information exposed or accessed in some way that would mandate a regulatory disclosure and a disclosure to consumers or investors. Here, what the SEC is saying, is that they expect a filing and a public disclosure that allows investors to make informed choices about their investments, even if a cyber event doesn't impact personal or sensitive information. So again, if it's reasonably likely to impact operations or security, then it needs to be reported.

Ken Fishkin: Is it okay for a company to file an 8-K and not be 100% sure if the disclosure is considered material or not?

Kathleen A. McGee: Yeah, I mean, that's what we're seeing. Notably, what we're seeing in these reports, are—I would say the vast majority of them—have acknowledged the cyber event is the result of a nation state actor getting access into their systems. And these are large tech companies, large health care providers. So, they are certainly something that you or I might say at first glance would be material. But the filings have been such that they're couching their terms—here's what's happening, we haven't yet made a determination that this is material. You know, further investigation and monitoring and perhaps further reporting.

And then we are seeing some updates to some of the original 8-K filings that can include things like public facing blogs or other disclosures, keeping the public informed, keeping the SEC informed, but still not saying that the event constitutes a material event. It'll be interesting to see how the SEC treats these filings in the long term, whether or not they end up issuing an advisory saying that those sorts of events constitute material events. But it'll be hard to penalize a company for making a filing, even if they say they don't think it's material, at least in this early phase. I think the question then becomes if you say it's material or if you say you're not sure that it's material, what does that really mean to an investor and how she's evaluating her investment?

Ken Fishkin: My final question is: what are some practical considerations that a company needs to take in order for them to be compliant with the latest SEC rules?

Kathleen A. McGee: First and foremost—and I know that we've preached it on this series before, Ken—it is so incredibly important to have policies in place, and so incredibly important to make sure that you're consistently reviewing and training on those policies. Administrative, technical, and operational safeguards have to be an inherent aspect to your policies. And now for publicly traded companies, you need to make sure that within your team, you've pulled together people that you've tapped to be the people to adjudicate whether or not something is a material event. And that needs to include people from IT, legal, and the executive, as well as any other stakeholders that you think are important.

Ken Fishkin: Well, thank you, Kathleen, this has been very informative. And thank you, everyone, for watching us on another episode of Lowenstein Sandler's Cybersecurity Awareness series.