Lowenstein Sandler's Cybersecurity Awareness Series

Session 10 – The SEC's Materiality Requirements: When is a Breach Considered Material Enough to Disclose?

By Kathleen A. McGee and Ken Fishkin
DECEMBER 2023

Ken Fishkin: Hello and welcome to another episode of **Lowenstein Sandler Cybersecurity Awareness video series**. Today, we're going to talk about the SEC's new rule that's going to effect on December 18th, where we talk about the materiality of a security breach.

Now, I know that the SEC now requires that material breaches be brought up after four days of knowing that there was a breach, but they really don't share any light about what "materiality" actually means. So, Kathleen, what are some of your thoughts about that?

Kathleen A. McGee: Well, it certainly popped everyone's balloon this season, I'll say. I think the biggest concern for companies is it's not just—to be clear, it's not four days from the breach or the security incident, it's four days from discovery that the incident is material. Significantly, a material incident doesn't have to be an incident that would traditionally be reportable under a state regime. For example, New York state or New Jersey data security law reporting requirements: here, the SEC's indicating that materiality is an incident or a series of events that impact the investor and their decisions on their investment.

So, it really could be something that would not traditionally be reported to government, but now has to be. And that is why a lot of—well, frankly, all of us—have been sent into a flurry. In point of fact, you can now have to report something, and by virtue of reporting it, make it a material event for investors, whereas before it just would have been a security bug that needed to be patched. I'm making that up, but you can see where I'm driving at here. You're putting it out to the public sphere, that is going to impact investors' decisions. In theory, whereas beforehand those security fixes would have happened behind a closed door, maybe the investor would have never known, and maybe that was okay.

Ken Fishkin: Last month, criminals got a little more sophisticated because they filed a whistleblower complaint with the SEC after they hacked the company. And I thought that was extremely creative and I wanted to know what your take on that was.

Kathleen A. McGee: I thought that was a brilliant criminal hat trick perpetrated by some ransomware actors. In big picture, the ransomware actor took a company for ransom. They weren't getting the attention that they wanted from that company, so they utilized the whistleblower function in a complaint form on the SEC to notify the SEC that they were in fact holding a company for ransom and the company hadn't told the SEC about it. I don't know what the outcome was, but suffice it to say, it just goes to show you how the best laid plans in these reporting regimes can have real unintended consequences for companies.

I think one big question that's out there right now in terms of these new materiality reporting requirements on security incidents is whether or not investors are actually going to know what really is actionable information and what isn't. The marketplace is already flooded with consumers getting data breach notifications on a regular basis. It's going to be interesting to make a sort of big picture determination. How do investors take information filed on the 8K about something that's disclosed as material and transform that into an action item based on their investments? Or do they just get overwhelmed and gloss over those things?

Ken Fishkin: Yeah, I could see that happening, especially if more and more companies are putting information into these 8Ks.

Kathleen A. McGee: Right, and you and I know, as people who have worked in this industry for a while, that, you know, the state limitations are for requirements on disclosures have always now hit a certain type of information that was considered private or sensitive information, whether it's health care or Social Security numbers or biometric information. But now the SEC is requiring that people get informed about security incidents that may not contain any of that information but may nevertheless be deemed material in some way. And so, I anticipate that is going to really flood the public marketplace with a lot of additional information. The question I have, though, is, is it really worthwhile for investors?

Ken Fishkin: What should companies do in general as far as measures to take to make sure that after they do get breached, what do they need to have in place?

Kathleen A. McGee: First, they should make sure that the policies and procedures that we've been talking about are in effect. If they are, then they will already have a communication strategy, a legal strategy, and probably an outside forensic IT company that's working with their cyber insurance coverage policy carrier to effectuate that first 24-48-72-hour plan to, you know, make sure that they understand what has been or could be implicated by a security incident; what information is out there that might be compromised; how they need to bring in legal counsel to evaluate whether or not something is material; and then lastly, how we're communicating both internally and externally. And unfortunately, now, once you've made that materiality determination, you've got four days. So, making sure that you have all these other things in place will allow

you a little breathing room—not a lot, but a little—to make those last four days go as swiftly as possible.

Ken Fishkin: Thank you, Kathleen, for this great information. And thank you for joining us for another episode of **Lowenstein Sandler's Cybersecurity Awareness video series**.