Lowenstein Sandler's Cybersecurity Awareness Series
Session 9 – SEC Proposed Cybersecurity Rules

By Kate Basmagian, Kathleen A. McGee, Scott H. Moss, and Ken Fishkin
APRIL 2023

Ken Fishkin: Hello and welcome to another episode of Lowenstein Sandler's Cybersecurity Awareness video series. Today we will be discussing the latest proposed SEC rules and their impact on public companies.

For this discussion, we have Kathleen McGee, a partner in the Tech and White Collar Criminal Defense practice group's; Kate Basmagian, Chair of our new ESG practice and partner in our Capital Markets & Securities practice; and Scott Moss, partner in our Investment Management group and Chair of our Fund Regulatory & Compliance group.

So, let's start with you today, Kathleen. The SEC now, since last year and even last month, has pushed down some proposed rules regarding cybersecurity disclosures and protecting consumer information. Do you think you can unpack it for us?

Kathleen A. McGee: Yeah, and it's a big deal, especially because of the signaling to public companies and investor management companies, the entire investment management community, about what this is going to mean for them going forward. So, as you mentioned, last year, the SEC announced they were going to be rolling out some proposed rules impacting the investor management community. They had already also unrolled some rules having to do with public companies writ large, they just put forth three new sets of proposed rules, and all of these are now open for a notice and comment period.

So, the actual enactment of these rules and the timeline is still unknown. That's important to know. Nevertheless, the focus of the SEC is twofold. First and foremost, they believe, and the Biden Administration has been really clear about this, that cybersecurity equates to national security. And so, the administration and the federal government is very concerned about all public companies maintaining strong cybersecurity.

Secondly, the SEC has announced in their proposed rules that they believe investors have the right to make important decisions based on, among other things, the quality of the cybersecurity of their investment vehicle. So, they're going to be able to take a look at public filings and other documents of prospective investments moving forward.

Ken Fishkin: That's great. So, that takes me to Kate. So, she talked about public companies being impacted on this. What's your take on that?

Kate Basmagian: Yeah, so, cybersecurity is definitely an area of focus for the SEC and also for investors, and in addition to these proposed rules, the SEC recently has also initiated some enforcement actions that are related to some misleading disclosures, and also disclosure control failures in the wake of certain cybersecurity incidents.

So, with these new rules, companies today should really be thinking about how to design and implement effective cybersecurity systems. And this is going to include also ensuring that they have proper communication channels set up, and disclosure plans, and also response plans. That's something that's going to need to be coordinated with their IT professionals, their management teams, probably some oversight by the board of directors, and if these new rules are adopted, they're also going to need a way to assess whether or not a particular cybersecurity incident is material, which that's going to vary by company. So, companies should really be thinking about what that means and what that looks like for them now.

You know, these new rules are not going to mandate that you have a cybersecurity expert on your board, but companies should always be considering the skills and assessing the skills of their directors, and now is a very good time to be thinking about whether or not to add someone with cybersecurity expertise to your board.

Kathleen A. McGee: I'm going to just add on to that, if I could, Ken. Several of the really notable features of these proposed rules are a potential for a 48-hour turnaround time on reporting what is considered a material issue with respect to data security; that's a very tight turnaround. Another issue that's been raised here is the potential for a up to two-year lookback period on any company that has to comply with these rules, which means that even if you don't have to be in compliance with the rules until they go into effect, at the time you have to come into compliance with these rules, the SEC has a right to look back two years into your prior operations with data security, which means that we're really recommending companies take a strong look at their protocols right now and see what they can do to enhance and document.

Ken Fishkin: Can you go a little bit more detail about why this is so important for investment managers to be able to shop.

Scott H. Moss: The SEC is essentially saying that they really, really care about information security, and privacy, and cybersecurity for everybody they regulate. So, that includes public companies–33 Act, 34 ACT registered securities–but it also includes financial institutions like registered investment advisors, and registered brokers, and registered investment companies that might be structured very, very differently from those public companies.

Now, it's probably not the first time they've ever thought about cybersecurity. An investment advisor, for example, that's registered federally will likely already have or has that already have a compliance manual, and this is just one part of it. And they typically cover privacy regulations at the state level and regulation SP already, but they're going to have to think about enhancing those policies and procedures. And if they're staffed particularly leanly, they're going to need to lean on experts in that area, because the chief compliance officer of these brokers or the investment advisers might be expert in various securities laws, but they may not be expert in privacy, or cybersecurity, and everything that they're hundreds and hundreds of pages of manuals have to cover.

Kathleen A. McGee: To expand on what Scott has just highlighted, notably some of these proposed rules impacting investor managers are also going to broaden the definition of the type of information that is considered reportable information.

So, traditionally, as you know, Ken, sensitive information was perhaps financial information, Social Security numbers, maybe even username and password, but the SEC is indicating that investors may have a broader sense of sensitivities around certain types of information that that the IM community could hold onto. And so, it will be interesting to see what the final rulemaking has to say about the types of information that are considered sensitive with respect to these rules. And that, of course, then goes and plays into what is considered material.

Ken Fishkin: Wow, that's a lot to take in. Thank you very much, Kathleen, Kate, and Scott. It's been a pleasure. And thank you for another episode of the Lowenstein Cybersecurity video series.