THE CONSUMER FINANCE PODCAST: SEC'S NEW CYBER RULES FOR PUBLICLY TRADED COMPANIES
HOST: CHRIS WILLIS
GUEST: KIM PHAN
POSTED: DECEMBER 21, 2023

Chris Willis:

Welcome to *The Consumer Finance Podcast*. I'm Chris Willis, the co-leader of Troutman Pepper's Consumer Financial Services Regulatory Practice. And I'm glad you've joined us today because we're going to be talking about the Securities and Exchange Commission's brand new rules on cybersecurity for publicly traded companies, which of course affects financial services companies and everybody else too. But before we get into that, let me remind you to visit and subscribe to our blogs, troutmanpepperfinancialservices.com and consumerfinancialserviceslawmonitor.com. And don't forget about our other podcasts. We have the *FCRA Focus*, all about credit reporting, *The Crypto Exchange*, which is about all things crypto. We have our privacy and data security podcast called *Unauthorized Access*, and our payments focused podcast called *Payments Pros*.

And all of those are available on all popular podcast platforms. And speaking of those platforms, if you like this podcast, let us know. Leave us a review on your podcast platform of choice and let us know how we're doing. And finally, if you like listening to and reading our thought leadership content, like our blogs and our podcasts, check out our nifty mobile app. It's a great place to get all of that content all in one place. You can even listen to the podcast from right inside the app. Plus it has a handy directory of our financial services industry group members and a handy calendar that shows what events and seminars we'll be presenting and attending. It's available for both iOS and Android. Just look for Troutman Pepper in your app store.

Now, as I said, today we're going to be talking about a new SEC rule that was adopted on July 26th, by a three to two margin, which basically requires public companies to do two things. First, it requires more immediate disclosure of a material cybersecurity incident, and then also as a matter of regular reporting, publicly traded companies will have to provide more information in their filings with regard to cybersecurity risk management and cybersecurity governance. And there's no one better that I could think of to talk to me and talk to you about these things than my partner Kim Phan, who's a member of both our Consumer Financial Services and Privacy and Cyber groups, and of course a familiar voice to listeners of this podcast. Kim, thanks for being on the podcast again.

Kim Phan:

Thanks for having me again. This is definitely a really exciting topic. And because it applies to all publicly traded companies, it's not specific to financial institutions, will certainly impact many of the larger financial institutions.

Chris Willis:

Well sure, because they have boatloads of personally identifiable information like perhaps no other industry does. Why don't you just take it from the beginning and let's talk about the breach piece of the

new SEC rules first. What information is a public company now required to report following a cybersecurity incident?

Kim Phan:

The new rules will now require that companies add in their Item 1.05 of their form 8-K, a disclosure of any cybersecurity incidents that are determined to be material. So a cybersecurity incident is broadly defined by the SEC, it's any unauthorized occurrence or series of related unauthorized occurrences. So a series of hacks versus one single attack, that is conducted on the SEC registrant's information systems that jeopardizes the confidentiality, integrity and security of either the system itself, or any of the information that resides in that system. And that disclosure has to describe a few specific things. It has to describe the material aspects of the cybersecurity incident, like the nature, scope, timing of what happened, as well as the material impact or what could reasonably result as a material impact from the incident. And materiality is a key issue here in the rule and materiality is anything that is determined to result in a substantial likelihood that the reasonable shareholder would consider it important when making an investment decision, or could significantly alter the mix of what information is available to shareholders.

And I point this out because the final rule attempts to focus mostly on just what material impacts there could be. Now, earlier versions of the rule had all kinds of other disclosure elements to it, but they've tried to narrow it down, to just would be the most material information a shareholder want to know about something that was going on at one of the companies that they're invested in. And the rule, and this was in earlier versions, but no longer requires a company describe what their current remediation status, like if they're currently under attack or where they are in responding to the incident. And they do not have to describe any of their internal processes or response plans to incidents which others had argued would give bad guys basically a roadmap to how to penetrate that same company in the future.

Chris Willis:

But still, even with those things omitted, it sounds like there's quite a bit for the public companies to have to report if there's an incident. When are the public companies required to provide these disclosures in relation to when the incident occurs?

Kim Phan:

That's one of the most challenging aspects of the rule, I think. All of this information has to be compiled and submitted to the SEC within four business days of the public company's determination that the incident is going to be material. So, not from the date of discovery. A company may be attacked and discover that they're under attack, but until they make the determination that attack has some sort of material implications for the company, that's when the clock starts running. And then once they make that determination, they can't delay unreasonably in providing notice to the SEC.

Chris Willis:

But still, I mean, four business days seems very rapid to try to make the kind of assessment of all the impacts and things that you mentioned in terms of what the disclosure requires. And it also seems to me that that four days could be while the attack is still underway and not yet completely resolved. I mean, think about a ransomware attack for example. It could go on for a week or more. Is there any leeway or flexibility to that four-business day deadline that you just mentioned?

Kim Phan:

This is one of the areas of the rule that has come under the most criticism, I think, from not just companies themselves, but other regulators that have taken a look at this rule. Because while many of the state data breach laws have a lot of flexibility with regard to say, law enforcement exemptions or other sorts of delays that might be appropriate, while a company is under attack and still trying to respond, there's a very narrow exemption from the four-day reporting deadline that is limited only to those scenarios in which there is a substantial risk to national security or public safety. And if there is, again, national security or public safety, the delay is only for 30 days. It is not indefinite as to when they are able to resolve some of those concerns. It's a limited delay, and in order to even get the exemption, you have to get written approval from the U.S. Attorney General, you have to go all the way to the top in order to get this exemption and to assert that exemption to the SEC, it is a very high standard to satisfy.

Chris Willis:

Okay. So it sounds like that exemption's going to be available only for those few times when a nuclear missile silo is hacked or something like that. Right?

Kim Phan:

Pretty much. And while the SEC has said that they're going to work very closely with the Department of Justice to set up some sort of process-

Chris Willis:

Oh, of course.

Kim Phan:

... That companies can take advantage of to communicate this to the Department of Justice, get the AG to weigh in.

Chris Willis:

Of course, yes.

Kim Phan:

Then communicate that to the SEC within those four business days. They say they're going to try to make it as easy as possible, but I mean, what can you really do in four business days?

Chris Willis:

Yes. When there are two federal agencies involved.

Kim Phan:

Yes. Two separate ones.

Chris Willis:

Yes.

Kim Phan:

Yes.

Chris Willis:

Okay. So I guess, chuck that out of the window in our minds I suppose. But leaving that sort of funny thing aside, you've told the audience about what the initial reporting obligations are within this four-day deadline that has no real exception to it, but what about after that? Are there ongoing reporting obligations for a public company related to an incident after that initial four-day report?

Kim Phan:

Yes. I think the SEC recognizes that a company might not have their full picture of what's going on within four business days. So after a public company makes the initial update, they can amend their Item 105 disclosure on the form 8-K when additional information becomes available. So there is some leeway there that while you do need to give the initial notification, there is additional time once additional information becomes available to make that amendment to your form 8-K. Now, the SEC, in a very significant change from actually the proposed rule to what they finalized, did not require other updates to previously reported incidents. It basically just says that you can add additional information but does not create a separate obligation to submit additional statements.

Chris Willis:

Well, that's interesting. What about a situation where the company reports an incident in the four business days that's required and then they later discover that the scope of the incident or the impact on the company is much larger than they initially reported? Is there no obligation for them to update to report that?

Kim Phan:

They are, the information that was required in the initial notice, right, material impacts that would be significant to a shareholder to know. If that information was not available at the time of the initial notice, they have to have amend, at a later time, but they don't have to provide additional information that wasn't otherwise required in the additional notice.

Chris Willis:

Okay. Understood. That makes that clearer to me. I feel like we've started this conversation on kind of a downer note by talking all about data breaches, which are kind of an unpleasant thing for people to think about. Let's talk about a sunnier, rosier part of the new rule, which is the ordinary course of business, and what disclosures are publicly traded companies now going to be required to make just in the ordinary course about their cybersecurity preparedness.

Kim Phan:

We have been talking about the form 8-K. This is an amendment to actually the Form 10-K, which adds a new item with regard to providing cybersecurity disclosures, so that public companies can understand how they're being managed and governing different cybersecurity risks. And these disclosures in this other form 10-K are generally focused around risk assessments, putting an appropriate governance program in place, discussing how those programs have evolved over time to reflect changing cybersecurity risks that the company may be facing, if they're rolling out new product, or if they're opening a new jurisdiction, or if they're updating their software. These are the types of material things that could impact the cybersecurity risk as a company. And so what organizations, public companies will now have to do is describe all those processes. How do they assess, identify and manage those material risks from various cyber threats that they may be facing.

And they need to provide that in a manner that the SEC describes as sufficient detail for a reasonable investor to understand. So not a ton of technical terminology or a bunch of other, very in the weed processes, but a high level overview. So again, the reasonable investor can understand what's going on, and it also requires public companies to describe whether any of the risks from various cyber incidents that they've reported, again, in their form 8-Ks, whether or not any of those have a long-term material impact on what the business strategy is, or other impacts on their operational status or financial condition. There's a whole list of other additional requirements. I don't know how detailed you want to get about some of these things, but it is not an insignificant burden to update their Form 10-Ks with all of this additional information that the SEC believes are appropriate for investors and other shareholders to have, about, again, the ins and outs of what a company is doing with regard to their cybersecurity program.

Chris Willis:

Well, let's just leave it at, there's a lot and then if the audience is interested in it, they can just ring you up or send you an email. Okay, Kim?

Kim Phan:

That sounds great.

Chris Willis:

One more question about data breaches. I guess I just can't get away from that. We know from experience that a lot of data breaches can occur with service providers. In other words, it's not the actual registrant's systems or like a bank's systems. It's those of a service provider and there's tons of service providers in the financial services world. How do the new rules accommodate for an event like that happening?

Kim Phan:

The new requirements do require that material incidents that involve a third-party system, that a public company uses such as a cloud provider, those are required to be reported as well. And while the SEC does acknowledge that the public company itself might not have a ton of visibility into that third party systems and what may be going on, again, their expectation is that the material impacts on the public company itself will be disclosed. And while the final rule generally does not require public companies to conduct additional inquiries and otherwise dig-down into the third-party service providers, the ins and

outs of their own systems, again, there is certain minimal information that the SEC is expecting that public companies provide to their investors and shareholders.

Chris Willis:

Okay. Does that mean, I guess, that once these rules become effective, now we're going to have to have a new contract term between publicly traded companies, financial services companies included, and their service providers who handle PII or other sensitive information, that the third party has to inform the public company within a very short period of time to enable it to attempt to comply with this four day rule? Right?

Kim Phan:

That's correct. And I should point out, Chris, that this will be something that companies need to start moving forward on pretty much right away. The final rule already went into effect. It went into effect on September 5th. The new disclosures are going to need to be incorporated into Form 10-Ks by December 15th of this year. New disclosures in the form 8-K are going to be required starting December 18th, and while some of the smallest public companies may have some leeway, they may be able to benefit from a timeframe that allows for an additional 180 days for them to get themselves in order. All public companies are now required to tag these disclosures under the final rule at the beginning of the year for their initial compliance with these disclosure requirements. It's a very short timeframe between today and the end of the year when many of these processes for reporting, not just data breaches, but also cybersecurity governance requirements, are going to need to be in place.

Chris Willis:

Okay. There's obviously a lot of considerations in both directions with respect to disclosures like this. You mentioned, for example, the need to provide information to investors versus the possibility of educating hackers essentially, on a company's cybersecurity defenses. In your view, did the SEC strike the right balance with these disclosures?

Kim Phan:

This was very controversial. It was pushed through with a vote of three to two, all three Democratic Commissioners on the SEC versus the two Republican Commissioners and chairman Gary Gensler, when approving the final rule, stated that he believed that the final rule will provide investors with more consistent and comparable information about companies they could potentially invest in, when making those decisions about relevant cybersecurity and cybersecurity incidents that may have occurred. But both of the Republican Commissioners, Hester Peirce and Mark Uyeda, dissented from the final rules. Peirce said that it creates a lot of uncertainty. She doesn't think that materiality is a good touchstone for disclosures. She's not sure where the SEC comes up with some of the authority for imposing these disclosure requirements on public companies. She believes that this is the SEC veering into business operations, dictating how companies need to be building out their cyber defenses, rather than simply serving in their oversight rule.

Uyeda, also similarly criticized that the SEC appears to be making decisions on behalf of investors, by elevating cybersecurity disclosures over other types of risks and issues that shareholders might care about more than whether or not a company's in breach. Because it's not if, but when every company is eventually going to experience some sort of breach and prioritizing these disclosures and information

could upset the scale that the SEC has previously determined is appropriate for these types of disclosures by public companies.

Chris Willis:

Of course, like it or not, we're stuck with it now, or at least stuck with it for the foreseeable future. Kim, I want to thank you for being on today's podcast and educating our listeners, including our many financial services clients who are themselves publicly traded on all these new requirements that they're going to have to come to grips with. And we're of course lucky to have you here to tell the audience about it and assist clients with issues like this that run the gamut of privacy and data security.

Kim Phan:

My pleasure as always.

Chris Willis:

And of course, thanks to our audience for listening as well. Don't forget to visit and subscribe to our blogs, troutmanpepperfinancialservices.com and consumerfinancialserviceslawmonitor.com. And while you're at it, why don't you head over to troutman.com and add yourself to our Consumer Financial Services email list. That allows you to get copies of the alerts that we send out when something interesting happens, as well as get invitations to our industry-only webinars. And don't forget to check out our mobile app. It's available for both iOS and Android. Just look for Troutman Pepper in your App store. And of course, stay tuned for a great new episode of this podcast every Thursday afternoon. Thank you all for listening.