Managing Cybersecurity Threats in 2024 Episode 2

PLUS Staff: [00:00:00] Welcome to this PLUS Podcast, Managing Cybersecurity Threats in 2024. You're listening to Episode Two. Before we get started, we would like to remind everyone that the information and opinions expressed by our speakers today are their own, and do not necessarily represent the views of their employers, or of PLUS. The contents of these materials may not be relied upon as legal advice. And with that, I'd like to turn it over to our host, David Shannon.

David Shannon: Thank you, Tyla. I appreciate it. And good morning or good afternoon to everybody who's listening. This is our second podcast this year. We started these last year, and for those of you that don't know, we try and give you some different policies, procedures, thoughts on all the different cyber security issues that are arising as we go through the year. There are a lot as everybody knows, but we try and pick out a few that are current and somewhat relevant to both the insurance industry and the public at large.

As Tyla said, I'm David Shannon. I'm a [00:01:00]shareholder at Marshall Dennehey, and I chair our cyber security practice and with me today, I have Ryan Friel, who's also a shareholder of the firm.

In our group, Ryan does a lot of work with financial institutions. He originally started working on SEC and FINRA investigations and defense work, and that has, of course, now gotten into the cyber field as well. And we're going to talk about some financial issues in SEC amendment.

But I'll just let Ryan introduce himself.

Ryan Friel: Good afternoon, Dave. Thank you.

Ryan Friel: I started doing cyber work with Dave about a year ago. Prior to that, I worked at FINRA as a regulator. So, I would deal with Regulation SP, which we'll be discussing today, but I would routinely go out to FINRA registered broker dealers and examine them for Reg SP compliance.

This topic today is particularly interesting to me with my background and looking forward to discussing with Dave.

David Shannon: Thanks, Ryan. And it's one of those where we're talking [00:02:00] about a regulation, it's not as maybe as fun and exciting as a good ransomware attack or something that's going on with one of the new threat actors.

But it is important, and I think it will get a lot more traction as companies over the next 2 years start to realize how they have even more notice requirements, more annual reporting requirements, things of that nature. So, I think it's important for not only companies and their shareholders, or their executive committees, or their IT companies to understand, but also in the insurance field, whether it be brokers, underwriters or claims professionals to understand what's going to go on over the next couple of years as the SEC starts to enforce this new amendment to this regulation. So, hopefully some people get some good ideas and some information from the podcast today.

Ryan, if you could just give us a brief description, explanation of what this Regulation SP is and how [00:03:00] the SEC amended it last month. And then once we understand what it is, we can talk a little bit about what it's going to entail for financial institutions.

Ryan Friel: Sure. So, Regulation SP or Reg SP for short, as it's known in the securities industry, was first instituted in 2000. Prior to this amendment, Regulation SP dealt primarily with safeguarding customer information.

I can recall doing examinations while at FINRA surrounding Reg SP and some of the concerns were precisely how FINRA registered broker dealers were preserving and safeguarding customer information in their offices. Whether they had, as silly as it might sound, the appropriate locking mechanisms on drawers and things like that.

Again, this was first instituted in 2000. On May 16th of 2024, the SEC adopted amendments to Reg SP, which substantially expanded the protections to the treatment of non-public personal information of consumers and really [00:04:00] creates a new standard for breach notification in the securities industry. Over that span of 24 years, the SEC has heightened the security requirements surrounding this set of information.

David Shannon: Yes, it shows you how slow the government is. It's taken 24 years for them to pass an amendment to this. But it's not surprising. And what we see in this field, unfortunately, is that the statutes and the regulations tend to be a little slow in keeping up with what's going on. I looked at it from our standpoint as privacy attorneys and for other individuals that are responding to

these type of events or are trying to prepare to be able to prepare to respond to them.

It looked like there was about 4 issues that were sticking out to me, one was you need to adopt more written policies and procedures about your incident response program. The second would be the notifications to customers. The third would be more record keeping about response programs, agreements with other entities.

And then the [00:05:00] fourth would be about implementing more changes to the annual privacy notices that are going out. Does that kind of, is that what you see too? These four broad areas that they've added to this amendment to add to this regulation?

Ryan Friel: Yes, there's a lot there, but I would say taking a broad look at, those are the four main areas of updated regulation.

David Shannon: And I looked at it from our standpoint, I think we're always going to look just as the privacy attorneys or whether it be the insurance underwriters or claims professionals about the impact on the notification issues. I saw a couple issues there that really jumped out at me--it seemed like the SEC is going to be a little more broad in the way they define either customer information, sensitive customer information as they refer to it, and the customer information then itself.

Would you agree it looks like it's a little broader than what we may see in some of the state regulations for data breach notices?

Ryan Friel: Absolutely. The customer information we're talking about and is even outlined in the amendment, [00:06:00] is broken into two categories. It's the information that can be uniquely identified with an individual.

So, there's social security number, date of birth, information like that. And then it also includes information that can be used to gain access to an account. So, there we're talking about username and passwords as well as answers to security questions.

David Shannon: And also, I forgot to bring up at the beginning, this would apply to, the way I understand it, to any SEC regulated entity, whether it's an investment advisor, investment companies, broker dealers, we could be talking about large companies, say, Fortune 500 banks or financial institutions as well as small individual brokers, correct, Ryan?

So it really affects everybody throughout the financial field.

Ryan Friel: It does, and the definition of cover institutions, which is the term that the SEC uses, was broadened in this amendment to include even transfer agents registered with the SEC or other regulatory agencies. So, when we're talking about transfer agents, we're [00:07:00] talking about trust companies, banks, or similar institutions assigned by a corporation for the purposes of maintaining investors' financial records.

The biggest transfer agent that comes to my mind, or perhaps the most well-known is ComputerShare. So, if you receive a financial document from ComputerShare, they're also now swept under this amendment.

David Shannon: Yes, and I looked at it, then if say you're talking, if you're in an insurance underwriter you'd really have to look if you have some of the large institutions, I think, obviously, are going to have an instant response policy and procedure. They're going to have these annual notices that they send out.

They probably have a lot of this work. They're just going to have to revise them a little bit. It's, to me, it's those smaller broker dealers whether it be, a one-person shop or even a ten-person shop. Those are the ones that really fall under this, they're going to have a lot more that they have to comply with when it comes to this regulation. Would you agree?

Ryan Friel: Absolutely. Prior to this amendment, there were no SEC rules that required broker dealers to have policies and procedures for [00:08:00] responding to data breach incidents. Yes, small or limited purpose broker dealers really need to start looking at their policies and procedures to get them to comply with this amendment.

David Shannon: And then, I talked a little bit about how the amendment is going to make everybody go back and look at their incident response programs and their annual notices and make sure that they comply with some of the SEC regulations on what they're notifying people about.

They'll have to put together an incident response program if they don't have it. I would suspect then that, and it'll take a few years, it would be if you have an incident and it's reported and if it's somehow reported to the SEC, they can come in just like you used to do and look at the lock cabinets, but they'll come in and want to see all these policies and procedures much like the way OCR does when they're doing an investigation for a healthcare covered entity that's had a breach.

Is that what you see coming down the line at some point?

Ryan Friel: Yes, absolutely. Smaller financial institutions like broker dealers need to [00:09:00] have policies and procedures that pretty much do three things.

The first is to assess the nature and the scope of any incident and to identify the customer information systems and types of customer information that may have been accessed. The second is procedures to contain and control the incident to prevent further unauthorized access. And finally, as you were alluding to, broker dealers must have procedures to notify affected individuals whose information was taken.

David Shannon: So, I think if you were to break it down even further these financial institutions, whether larger, small, have a lot more of record keeping they're going to have to do now. And that's going to have to be there if there is an incident response and you've got a regulator that's doing investigation in some way, shape or form.

A lot like we've developed with the health care providers with HIPAA, high tech, and everything that they have to do and be able to provide and probably down the line. It'll take a few years, but we might start seeing letters, if the SEC starts making [00:10:00] people report these to them they may come back and start doing that too. We'll have to see.

The other issue I just wanted to hit on then for those that are listening that are more involved in the actual notifications, is really looking at the notification requirements. Because, all of a sudden now you have a notification requirement that's in this regulation, so it may be where you were going to notify anyway, because you had obligations under state regulations, but now you definitely have a, if you're a financial institution, you've got an obligation under this amended reg to notify as well that's correct, right, Ryan?

Ryan Friel: Yes, absolutely. There's a presumption of notification under the amendment. A covered institution may choose not to notify if following a reasonable investigation, establishing that customer information has not been or is not reasonably likely to have been accessed, but there is a presumption of notification under the amendment.

David Shannon: That's the way I looked at it, too. And that's why I mentioned at the beginning that I think that there are definitions for personal information and for sensitive [00:11:00] customer information are much broader than we'll

see in a lot of the state regs, so that if you're a financial institution, you're going to look, say, at your state regulations, whether it be California, New York, et cetera.

But you may then have to, and I think not may, but will have to look at this regulation and say, under this definition of sensitive customer information or customer information, do we have a requirement to notify as well? And I think that the legal analysis will likely say that you do, and they even have a timing in there that they're saying it needs to be done no later than 30 days.

Now, there's other regs that the financial institutions have to comply with that may say that shorter anyway, but at a minimum, I think you're now looking at, you're going to see privacy counsel telling their clients that are financial institutions that, you've got some sensitive customer information and you've got to get notices out within 30 days.

That's the way it looks to me. And they even give some indication of what they want in the customer [00:12:00] notifications as well, Ryan?

Ryan Friel: Sure. There's no specific method of notification. However, the SEC says notice must be transmitted by means designed to ensure that the affected individual can reasonably be expected to receive actual notice in writing.

And when we're talking about the areas that they want to identify, we're talking about nature and date of the incident, the data involved, as well as the contact information for the covered institution. So, the customer can easily contact the financial institution to get more information.

David Shannon: And one of the little things I said, there's so much in this that'll have to be played out and played with by the attorneys and the financial institutions and the carriers as well. But I saw, the way I read it in some respects was they were saying, if you can't determine whose customer information was accessed, you have to provide notices to all individuals.

Whose information resided on that system that was accessed, say, by a threat actor? Now we do that in a lot of instances anyway, if we can't fully determine, but they're really laying it out that if you can't tell [00:13:00] us, whose information or what file was accessed by a threat actor, then you've got to notify everybody on that server or on that system, depending what you can narrow it down to.

And that can get expensive because some of these financial institutions can have a lot of people who may have to get notices, right?

Ryan Friel: Yeah. It's interesting. The covered customers on those amendments, as you're saying is extremely broad cover institutions are expected to notify individuals even those that don't have a customer relationship with them.

So, this includes any information for customers received by covering institutions from third party financial institutions like a transfer agent. So yes, it's very broad.

David Shannon: I think that'll be something that we'll really have to look at, because we're always trying to narrow down who we need to notify, can we say it's a non-notification incident but when that's pretty broad, when the definitions are pretty broad for how you're defining what customer information is or sensitive information as they refer to it [00:14:00] we may see, it'll take a few years, but we may see them really coming down more that they want notices going out.

And I know in the statement that was released with this amendment, the SEC chair even pointed out that they were now introducing a notification requirement into their safeguard rule for this regulation. It's going to take, what, a couple of years for this to be fully instituted Ryan?

I think it was the smaller institutions that had a little longer until they had to comply as compared to, say, larger ones.

Ryan Friel: Sure, large entities have 18 months. The SEC defines a large entity as one having net assets of 1 billion or more at the end of the most recent fiscal year. And the smaller entities have 24 months.

Yes. Financial institutions need to really start ratcheting up their policies and procedures to be able to comply in the short term.

David Shannon: I think that's the takeaway, at the end of our discussion, really, is that over the course of the next 18 months to 24 months, the financial institutions, I think, need to review all of their [00:15:00] policies and procedures when it comes to customer information and IR responses their agreements with other entities on who's maintaining and safeguarding the data and more importantly, who's responsible if notices have to go out.

So, I think we'll see a lot of that from financial institutions. And then in 2 years, when these financial institutions inevitably start to have breaches, it will be, how are the privacy attorneys and in effect the insurance carriers, how are they going to deal with the notifications?

Are we going to see a lot more broad notices because of these kind of broad definitions in this rule? Or is it going to play out that on most of these under the state regs, you would have been notifying anyway? So, this is just one more regulation you're looking at, but you would have been notifying whether you had this amendment or not.

We'll have to see how that plays out and what that does for not just the institutions themselves, but the attorneys and the carriers on how they're going to respond to these [00:16:00] incidents. Any final thoughts there, Ryan, before we end this? I think we covered a lot there. There's a lot in these amendments, and we'll have to see how it goes.

Ryan Friel: There really is. I think as always, especially with the FINRA regulated entities they should be striving for reasonableness in their policies and procedures and in their incident response program.

David Shannon: All right. Thanks, Ryan. Appreciate it. And thanks, Tyla, and everybody for listening and we'll get you another one in a few months as well.

See what comes down the pike in the cyber world over the summer months.

PLUS Staff: Thank you for listening to this PLUS Podcast. If you have ideas for a future PLUS Podcast, please complete the Content Idea form on the PLUS website.