Consumer Finance Monitor (Season 4, Episode 48): A Close Look at the Final Rule Requiring Notification of Ransomware and Similar Computer-Security Incidents Issued by the Office of the Comptroller of the Currency, Federal Reserve Board, and Federal Deposit Insurance Corporation

Speakers: Chris Willis, Phil Yannella, and Kim Phan

Chris Willis:

Welcome to the Consumer Finance Monitor Podcast, where we explore important new developments in the world of consumer financial services, and what they mean for your business, your customers, and the industry. I'm your host Chris Willis, the co-leader of Ballard Spahr's Consumer Financial Services Practice Group, and I'll be moderating today's program.

Chris Willis:

For those of you who want even more information, don't forget about our blog, consumerfinancemonitor.com. We've hosted the blog since 2011 so there's a lot of relevant industry content there. We also regularly host webinars on subjects of interest to those of us in the industry. So to subscribe to our blog or to get a on the list for our webinars, please visit us at ballardspahr.com. And if you like our podcast let us know, leave us a review on Apple Podcast, Google, or wherever you get your podcast.

Chris Willis:

Now, today we're going to be talking about a new federal banking agency rule requiring notification of computer security incidents. And I'm joined by two of my partners who are very, very well qualified to talk about that. I'm joined by Phil Yannella, who is in our Philadelphia office, and Kim Phan, who's in our Washington DC office, and both of them are in our privacy and data security group, and both of them specialize in providing privacy and data security advice to our consumer financial services clients. And so we're going to be talking about this final rule today.

Chris Willis:

So both of you welcome to the podcast, and thanks for being here. And Phil, let me start with you in terms of asking you about this rule. What's the background on this new joint agency final rule? I mean, what prompted the federal banking agencies to make these changes?

Phil Yannella:

Well, first of all thanks Chris, it's great to be here. To answer your question the simple answer is ransomware. Although the final rule that was promulgated by the agencies is actually a little bit broader than ransomware, there's no question that the motivating factor behind the promulgation of the rule was the scourge of ransomware, which over the last three years has become a major problem for corporate America. Studies have shown that in 2020 U.S. companies paid almost a billion dollars in ransom to threat actors to try to get their data back. Ransomware has been a major problem for pretty much every industry in the country, but banks and banking service providers have been hit particularly hard. So given the frequency and the severity of cyber attacks in the financial services industry, the various agencies that promulgated this rule, and that would be

the Federal Reserve, the FDIC and the OCC, believe that it was important that a banking organization's primary federal regulator be notified as soon as possible about what we're going to call significant computer security incidents. I'm using air quotes and I'll define what that means a little bit later.

Phil Yannella:

But they are major security incidents that disrupt or degrade or are reasonably likely to disrupt or degrade the viability of a banking organization's operations. The agencies believe that timely notification was important to allow them to have early awareness of emerging threats to banking organizations into the broader financial system to better assess the threat that a notification incident poses to the banking organizations, to facilitate and approve requests from banking organizations for assistance through the U.S. Treasuries Office of Cybersecurity and Critical Infrastructure Protection. To provide information and guidance to banking organizations, and to conduct horizontal analyses to provide targeted guidance and adjust supervisory programs. Because of all this the agencies issued a proposed rule at the end of last year, in December of 2020. There was a 90 day period to obtain comments from folks in the industry, which they did. They pulled all those different comments together and they just announced the final rule in middle of November.

Chris Willis:

Thanks, Phil. And so in broad strokes what are the new requirements of the rule as applicable to banks and obviously bank service providers as well?

Phil Yannella:

Well there's really two main new responsibilities that are announced under the final rule. One involves banking organizations and the second is for service providers, and I'll start with banking organizations.

Phil Yannella:

The final rule requires that covered banking organizations are required to provide notice to their primary federal regulation where a notification event occurs. Now a notification incident is a computer security event that results in actual harm to the confidentiality, integrity, or availability of information, or an information system when that occurrence has or is reasonably likely to materially disrupt or degrade, and there are three things that follow from that.

Phil Yannella:

A banking organizations' ability to carry out banking operations or deliver banking products, that would be one trigger. The second would be an event that materially disrupts or degrades business lines, the failure of which would result in a material loss of revenue, profit, or franchise value to the bank. And then the last is an event that materially disrupts or degrades the operations, including associated services, functions, and support, the failure or discontinuance of which would pose a threat to the financial stability of the United States. So if a banking organization has an event that meets that requirement, meets the definition of a notification incident, the new rule requires that they notify their primary federal regulator as soon as possible and in no event more than 36 hours after the occurrence of that incident. Okay, so that's the first part of the final rule. And that again applies to banks.

Phil Yannella:

The second part of the rule is a notice for requirement that applies to a bank service providers. And what that rule says is that bank service providers have to notify at least one bank designated point of contact as soon as possible when the bank service provider determines that it is experienced a computer security incident that has or is likely to materially disrupt or degrade covered services for more than four hours. So basically it's the same rule that applies to banking service providers. The one difference is that for banking service providers they have to provide that notice if they believe the event is likely to last more than four hours. And their requirement is to notify their banks, their customers, as soon as possible.

Phil Yannella:

Now one of the questions that of course comes from this new rule is what exactly is a banking service provider? And what the new rule says is that a banking service provider are those service providers which under the Bank Service Company Act provides the services covered by that rule. Now the BSCA is sort of an older rule that some of our listeners may not be that familiar with, but the BSCA requires depository institutions to notify in writing their federal banking agencies of any contracts and relationships they have with technology service providers that provide certain services. And the covered services include check and deposit sorting and posting, computation and posting of interest, preparation and mailing of checks or statements and other clerical bookkeeping, accounting, statistical, or similar functions such as data processing or online banking. This rule, the BSCA would cover a lot of fintechs and a lot of cloud providers, so if you're an entity out there that falls into that general rubric then you're going to be covered by this new rule.

Chris Willis:

Phil, you noted that the agencies have gone through a notice and comment rule making process with respect to the rule as they would be required to do under the Administrative Procedure Act. Can you tell the audience how the final rule compares to the proposed rule? And it's always interesting to see did the rule get better or worse from an industry standpoint between the proposed rule and the industry rule? So how did we come out on this one?

Phil Yannella:

Well, I'll tell you that the agencies received 35 comments. And the vast majority of the comments that they received were actually pretty favorable. Most commenters felt that this was a good rule and it was a rule that would help fill in some of the gaps that currently exist in breach notification rules. Right now most banks and banking organizations and their service providers are really... There's two kind of rules that cover breach notification. There could be rules under the Bank Secrecy Act, and there's also existing inter-agency guidelines that really are meant to cover the breaches of personal identifiable information. There really wasn't a rule that specifically covered ransomware. So most commenters felt that this was a good rule and it would help fill in gaps.

Phil Yannella:

There were a lot of comments about different proposals, and I'll go through some of them. I would say overall the changes that were made to the proposed rule and what ended up in the final rule are an improvement over where they were in December of last year, and I'll give you one example. In the initial rule the definition of a computer security incident required only potential harm to the confidentiality, integrity or availability of the system. And in the final rule they changed that from potential harm to actual harm. So that's actually in my view an improvement for the industry.

Phil Yannella:

The proposed rule back in December, 2020 also included a provision that would have included violations of any internal policies or procedures. That would have qualified as a potential notification incident. And that provision was stripped out of the final rule.

Phil Yannella:

Some other ways in which I think the rule was improved from the initial rule, initially the definition of a computer security incident included the words could in good faith materially disrupt, degrade, or impair the viability of bank operations. So there was some kind of loose, fuzzy language that some commenters brought up, and ultimately in the final rule they took out could and in good faith and they replaced it with a reasonable likelihood standard, which is a little more objective and easier to apply.

Phil Yannella:

A couple other important changes, in the original proposal service providers would have been required to immediately report a notification event. That was loosened up a little bit so it went from immediately reporting to as soon as possible.

Phil Yannella:

Also in the original proposal service providers would have been required to report a security incident to two bank contacts. That was changed in the final rule and it was in the final rule you only have to now report the notification event to one person at a bank. So that's an improvement.

Phil Yannella:

Overall I would say in the final rule they did keep most of the original proposal but the changes that they did make I think are going to be easier for banks and for server providers to apply.

Chris Willis:

Thanks, that sounds like there was a very reasonable consideration of the comments as part of the rule making process, and that the changes were really quite rational. That's really great to hear.

Chris Willis:

Now Kim, let me turn to you. I mean, Phil made this rule sound kind of simple, you have an incident, you have a red phone to your bank regulator, or your bank if you're a bank service provider, you pick it up and you report. So from a compliance perspective is it all just peaches and cream here or are there any difficult or controversial parts of this new rule from a compliance standpoint that banks should know about, and their service providers?

Kim Phan:

Well yes, I would say the rule itself is not peaches and cream in any way. And Phil certainly laid out very clearly what the expectation is and how companies should be thinking about complying.

Kim Phan:

But while the regulators did take into account some of the comments and made as I agree with you very reasonable changes to reflect some of those comments, the underlying requirement itself is where the challenge lies, right? So at least some of the commenters, and I would probably say most of the commenters, would have noted that 36 hours is a very, very short window of time. Even the European Union's General Data Protection Regulation and the New York Department of Financial Services Cybersecurity Regulation, both of those, which are considered some of the most stringent requirements imposed on any companies, not necessarily just financial institutions, as being the most stringent in the world right now. The federal regulators here, the Prudential Regulators and the financial system took that a step further and shaved that in half, 72 hours down to 36. So that alone is a very dramatic change and a shift from where I think other regulators are in this space. So that will be incredibly challenging for many financial institutions to try to turn around a notification in that short period of time.

Kim Phan:

Now, the regulators in their commentary to the final rule did note well yes we have this very short window of time, but we don't think it will be burdensome on supervised entities under each of these federal regulators, the OCC, the FDIC and others because the notice is simply that, you just have to let us know. There's no content requirement as far as what that notification has to say. You don't have to tell us what's going on, how it's happening, the root cause, you don't have to have any of that analysis done by the time you let us know, we just need to be aware so that we can do our analysis, do their horizontal review.

Kim Phan:

And then as Phil noted they potentially could require an entity that has provided this notice to make changes to their program to reflect what's going on with the incident. So the regulators seem to believe that this is reasonable, but because of the minimal content requirements of the notification, but that 36 hour window, there's so much that happens in that period of time that it will be a challenge no matter what for any entity and specifically these financial institutions to try and satisfy.

Chris Willis:

So what should banks and service providers do from a practical standpoint? I mean, we've got this very difficult to meet requirement in terms of notifying the regulators so rapidly when an incident is just starting to maybe unfold perhaps, and you may not even know that much about it. So from a practical matter what should banks and their service providers do with an eye towards future compliance with this rule?

Kim Phan:

Sure. And I would have to say preparation is absolutely critical here. And I would flag that that 36 hours is at most 36 hours, right, so the regulators have even said in the rule we want you to let us know as soon as possible, but no later than 36 hours. They even say that for some of the most critical incidents they're expecting a same day notification. So the 36 hours gets even shorter when you're thinking about some of the criticality of some of the potential instance that these companies may be facing.

Kim Phan:

And so I guess the idea would be that companies have to be absolutely ready and should be thinking about how they're going to build out their processes to reflect this. The rule helpfully offers some examples of the types of notification incidents that they're expecting to receive notice of in these 36 hours, incidents like a distributed denial of service attack that disrupts customer access for more than four hours, attacks that impact core banking platforms that result in widespread system outages, failed system upgrades or changes, pretty much any incident that involves the activation of a financial institution's business continuity or disaster recovery plan, as well as Phil flagged, malware, which is specific to ransoms. Asking for ransoms that impact either core banking systems or backup data.

Kim Phan:

So to the extent that companies have internal policies and procedures or instant response plans, they should absolutely be updating them for those specific examples that are provided.

Kim Phan:

They should also be thinking about the types of critical incidents that would meet this threshold that Phil described that would be a notification incident. That way they're not trying to struggle with that determination within that 36 hours, is this or is this not a notification incident?

Kim Phan:

They should have appropriate training on any updates they make to their policies and procedures in this regard, such as many companies do tabletop exercises, which are real life, simulated exercises that try to play out the changes they may be making to their incident response plans. That might make sense. They might want to have additional processes that they want to build out to try to meet this requirement, as well as again of course keeping good relations with their credential regulator.

Kim Phan:

But some of the other things that are flagged in just these examples, like the example to the change management of a company systems, right? If you are onboarding a new technology, or maybe you're about to launch a new functionality, it will be critical to really test those systems in advance and build out your change management processes, because if there is an incident you now have this notification requirement. So there's a lot that these financial institutions have to be doing in house, but then you add the service provider aspect, which Phil described, right?

Kim Phan:

The reality is that this downstream requirement to have your service provider notify the financial institution, so the financial institution can notify their regulator, has to be built out into your contractual obligations, right? So looking back through all of

a financial institution's contracts with mission critical service providers, not every service provider but certainly the mission critical ones, and ensuring that those downstream obligations are in place and that there's a process. If the service provider notices financial institution, how they assess that to provide notification to the regulator. So while the regulators seem to think this will not be a burdensome process to comply with, it actually in reality will require quite a bit of thoughtful planning and steps taken in order to comply.

Phil Yannella:

Yeah, and Chris if I can jump in on that, one thing we shouldn't lose sight of is lots of banks are using vendors who are themselves using subprocessors, who themselves may be using further sub-processers. So if your a bank and you're giving your data to a vendor it very likely could be three or four steps removed from the bank at the end of the day. And you have to be thinking about all of those contractual relationships, because each one of those service providers is going to have to be in a position to provide upstream notice as soon as possible if there's a notification incident.

Phil Yannella:

And the other thing I think this is a little provision that maybe we'll get lost so I'm going to try to highlight it, I mentioned earlier that in the original rule service providers had to give notice to two folks, two contacts at a bank, and they stripped that back and they said it only has to be one contact at a bank. But there's another part to that, and that is if the contract doesn't identify who that designated person is in a bank the final rule says that the service provider has to notify the CEO and the CIO of the bank. So one of the things that everyone should be looking at when they go back and re-review these contracts is to make certain that a designated person is identified in the contract. Otherwise, service providers are going to be calling your CEO, which could be less than ideal.

Chris Willis:

Now there's one further question that I wanted to cover with the two of you before we sign off from today's episode, and that is the subject of your blog. I mentioned the Consumer Finance Monitor Blog at the beginning of the podcast, but you as our privacy and data security group also have your own blog, so would you mind telling our listeners about it so in case they're interested in privacy and data security developments, which they will be since they're listening to us right now, they can know a way to keep up with that through your blog.

Phil Yannella:

I'd love to. We've got a blog, it's Cyber Advisor, which is www.Cyberadvisorblog.com. We blog pretty regularly on data privacy and data security events that are of interest to our clients. The promulgation of the final rule is one of those events. We posted a blog post on it last week, so everyone can take a look at that. We do cover big events that are relevant to the financial services industry pretty regularly. I think it's a great resource and recommend that everyone check it out.

Kim Phan:

Yeah. And if I may, while Ballard does make a great deal of free content available to our clients and to others in the industry, I did want to flag that we also have a paid subscription service that we make available to anyone in the industry who is interested. It is our privacy and data security tracker, it follows very closely specifically for the consumer financial services industries, developments in privacy and data security.

Kim Phan:

As part of that subscription you receive a weekly email that covers all of the privacy and data security developments that have happened on both a federal and state level over the past week. At the end of the month we have a monthly round table call with all of our subscribers so that we can discuss trends and highlight other developments that we flag throughout the month. And then finally there is an online portal that's available to our subscribers 24 hours a day, seven days a week, 365 days a year,

where you can look up specific items where we post legislation, new regulations, all types of interesting items there. So if anyone is in interested in that I would encourage you to reach out to me, I would be happy to tell you more about it.

Chris Willis:

Thank you very much Kim for that. And thank you both Phil and Kim for being on the podcast today and sharing your expertise and knowledge regarding privacy and data security in general, and this new final rule about breach notifications.

Chris Willis:

And to our listeners thank you for listening. Be sure to visit us at our website ballardspahr.com, where you can subscribe to our podcast in Apple Podcast, Google, Spotify, or your favorite podcast platform. And don't forget to check out our blogs, Consumer Finance Monitor, and Cyber Advisor for daily insights about the financial services industry and privacy and data security. If you have any questions or suggestions for our show please email us at podcast@ballardspahr.com. And stay tuned each Thursday for a great new episode. Thank you all for listening.