Consumer Finance Podcast – Privacy and Data Security Update
HOST: CHRIS WILLIS
GUESTS: RON RAETHER AND KIM PHAN
POSTED: OCTOBER 13, 2022

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 we have a great podcast for you today on all things privacy and data security. But before we jump into that, let me remind you to visit and subscribe to our blog, consumerfinancialserviceslawmonitor.com, and don't forget to check out our other podcasts. We have lots of them. We have the *FCRA Focus*, focused on credit reporting, *The Crypto Exchange*, on all things crypto, and *Unauthorized Access*, which is the podcast of our privacy and cyber group, and all of these are available on all popular podcast platforms online. And if you like our podcasts, let us know. Leave us a review on your podcast platform of choice.

Now, as I said today, we're going to be doing a general update on privacy and data security issues, and I'm really pleased to be joined by two of my partners from our Privacy + Cyber Group. We have Ron Raether, who's the co-leader of that group, and Kim Phan, who's a partner in that group. So, Kim, Ron, welcome to the podcast and thanks for being here today.

Kim Phan:

Chris, thank you for having us. Always happy to be here on your podcast.

Ron Raether:

It's pleasure to be here, Chris. I appreciate it.

Chris Willis:

I'd like to talk to you, and have you talk to our listeners about generally, what's going on with privacy and data security, and Kim, let me start with you with some sort of regulatory updates. In consumer financial services, we're used to the CFPB being the most active regulator on most issues, and the CFPB of course has done that on a broad variety of issues but generally hasn't been in the forefront when it comes to privacy type issues and data security issues. Is that something that we should expect to stay the same or might it change under the current administration?

Kim Phan:

It's actually been really surprising for the entire course of the CFPB's existence that they have been so quiet on privacy and data security. They've always had the authority to pursue that area under their general UDAAP authority, Unfair and Deceptive Abusive Acts and Practices, but they really just haven't done a lot in that area. They had an enforcement action against Dwolla, a payment processor a few years ago, and that was a deceptive claim. But otherwise, the CFPB has been very quiet on this issue, and I think we can absolutely expect that changes. That was something that we had predicted because Rohit Chopra, who has now taken over as the director at the CFPB, was formerly an FTC guy, and at the FTC, he was very strongly

advocating for privacy and data security consumer protections. He was one of the dissenting voices to the Facebook $5 billion consent order because he thought it didn't go far enough.

So, we had already expected the CFPB to make this shift and they've come out swinging. They have issued a new data security circular that communicates their expectations with regard to data security at financial institutions and their interest in bringing enforcement action to that area. And while it isn't as broadly written as some of the guidance that we've seen come out of the FTC, it is focused on data security generally at financial institutions as well as at their service providers. And it calls out three very specific data security practices that it'll be looking at especially. One is multi factor authentication and the ability of financial institutions to protect consumers' personal information, whether or not it's being accessed internally by employees, externally by actual customers or third parties that may have access to that information, they're looking at MFA, multifactor authentication, across the spectrum.

They also address password management, and to the extent that companies are still using passwords. There's been of course a lot of interest in getting away from passwords because the reality is they're really not that secure. And while the CFPB doesn't go that far, say that passwords should be retired, it does say that they need to be properly managed. And one of the things that I've found interesting in their circular is not only do companies have to worry about managing their own passwords, but they need to actually be monitoring other entities to the extent that those entities have breaches that could be compromising the passwords that their own employees or that their customers are using to access their own financial information.

And the last area that's touched on by the CFPB circular is software updates. The reality is if you're using softwares, and every company uses external as well as internal softwares, those softwares constantly need updating for security purposes as vulnerabilities are found and other issues are being resolved, and that companies need to be on top of updating their softwares that they're deploying in their operations.

So those are the three that the CFPB specifically called out, but I think that is not in any way should be considered the limits of what the CFPB will be looking for when they're trying to identify potential security risks to consumers' information.

Chris Willis:

That's a really interesting development with the bureau wading into the fray. Of course, Kim, you mentioned while you were talking about director Chopra's background that he used to be at the FTC, and I've always thought about the FTC as being the de facto lead privacy and data security agency in the US because it had been the most active of the federal agencies. What's the FTC been doing lately on this front?

Kim Phan:

So, the FTC interestingly is doubling down, right? So much of what the FTC's consumer protection authority was taken by the CFPB when the CFPB was created, and while the FTC continues to have some enforcement authority there, privacy and data security was very much their safe space, where they were comfortable, where they brought a lot of activity, and I think they're stepping up their game at the same time that the CFPB is doing so, and I think that is not coincidental. I think the CFPB, and the FTC are working much more closely together based on Chopra's relationships there, as well as Lina Khan, who has now taken over as the chair, is very interested in these issues, as well as the fifth and final commissioner that fills out the

commission, Alvaro Bedoya, who was confirmed last year. He's a long term-privacy advocate, so it's very clear that this has been and will continue to be a major focus of the FTC.

And with the reality of Noah Phillips, who has recently announced that he's resigning, the FTC is going to be much more aggressive because now, the commission will be comprised of three Democrats and only one Republican once he steps down, so I think they'll be able to push through some very aggressive things, and the FTC is moving very quickly forward on a lot of different initiatives. One directly applicable to our financial institution listeners is the reality that the GLBA safeguards rule update, which was updated for the first time in close to 20 years, will go into effect as of December 9th. We're a little over a hundred days away from that effective date, so to the extent that companies haven't been paying attention to that, they need to be because it requires some pretty complicated operational changes.

Again, multifactor authentication is something the FTC flags in that update, encryption, logging, updating service provider contracts, as well as having a designated qualified individual. And we can expect further changes to the safeguards rule because the FTC already announced that they're considering whether or not to require financial institutions to certify on an annual basis that they're complying, and/or report any kind of data breaches to the FTC.

I would say the biggest change though happening at the FTC is their new rulemaking. They're engaged in a privacy rulemaking, not under their Section 5 UDAAP authority but under their Section 18 trade regulation rules. And that privacy rulemaking will be broad ranging. They characterize it as commercial surveillance but that is a misnomer in every possible way. Companies across every industry, not just the financial services industry, have to be worried about this because it addresses any business that is collecting, analyzing, and selling any type of personal information from consumers. So, it will be broad ranging. It's yet to be seen where that goes, but it will almost certainly have an impact on everyone listening today.

Chris Willis:

Lots and lots of action on the regulatory front, but let's not leave out legislatures across the country because this is an area where there's been a lot of legislation in recent years, like in California for example. Is there any upcoming privacy legislation that we need to be concerned about?

Kim Phan:

Concern is an interesting word because during the press conference the FTC had about its privacy rulemaking, the commissioners all said essentially that if there was federal legislation in this space, they wouldn't be doing this privacy rulemaking. And Bedoya, the newest commissioner, even said that if federal legislation is enacted in the interim during their privacy rulemaking, he will vote against the privacy rule making when it's finalized because he wants to defer to the legislature on this. So that's an interesting point with regard to how the FTC rulemaking might proceed. But for now, the biggest movement on the federal level to implement privacy legislation is currently the American Data Privacy and Protection Act. It is a bipartisan bicameral bill that was introduced by the two leaders of the House Energy and Commerce Committee, Frank Pallone and Cathy McMorris Rodgers, as well as the ranking member of the Senate commerce committee, Roger Wicker. The only person they didn't get onto that bill was Maria Cantwell. She's the current chair in the Senate Commerce Committee.

Right now, that bill has moved quickly. It was introduced this summer. It has started moving through the House. It has been approved by the subcommittee, reported out by the full

committee, and it's an open question whether or not it'll proceed to the House floor. I think the biggest hurdle that bill will face is in the Senate, if it gets out of the House. Schumer has already made clear that he's not moving any bills to the Senate floor that don't have a 60 plus filibuster proof majority, so unless Maria Cantwell changes her mind with regard to this bill and her big issues with this bill or with regard to the consumer private right of action as well as state preemption of more restrictive privacy laws like California, that this probably won't move, but we'll be keeping a close eye on it.

But the main activity as you noted is all in the states. The California CCPA will be amended by the CPRA the California Privacy Rights Act, at the end of the year. The new California Privacy Protection Agency, the first of its kind in the country which was formed earlier this year is moving forward with its rulemaking. Some of the other states that have comprehensive privacy laws, Virginia, Colorado, Utah, Connecticut. Some of those also have rulemaking that will be implemented. Colorado's attorney general recently announced that he's going to be having some listening sessions with the public to try to see how those rules are crafted. So really, a lot of the privacy activity as far as legislation and regulation is happening on the state side. And don't forget, the states can enforce the Consumer Financial Privacy Act. The CFPB has made clear that they have the capability to do that so to the extent that they want to bring enforcement actions under this new CFPB circular, they could do so.

Chris Willis:

That is a bewildering amount of activity, Kim. Thank you for that regulatory and legislative update. But Ron, I want to talk with you about the litigation side. When it comes to privacy and data security, what are the recent litigation trends that our listeners should be paying attention to?

Ron Raether:

One of the things I want to pick up on is what Kim was saying. We know we've heard from the CFPB for example that they intend to be more aggressive and litigate issues, and so frankly, it will be of value to me to see exactly if they follow through on their word and what that will mean in terms of our clients and the litigation that we're seeing. So, for example, there are questions about from an administrative law perspective, does the CFPB, or in particular what Kim was saying about the FTC, does the FTC actually have the authority to create the regulations that go to specifics on cyber security or privacy. The ADPPA has a provision in it that would give rulemaking authority to the FTC, which to me begs the question, why is that necessary if they think they already have the authority? That regulatory litigation I think is going to be interesting, Chris, and seeing how that develops over time, as well as what we're seeing, for example, in California.

California's been very slow to do anything other than informal inquiries. I suspect at some point that there will be litigation, but in turn, what does the regulatory litigation do in terms of what we're seeing from private plaintiffs and plaintiff's firms? And what I will say is we're seeing a wide variety of things. So, everyone is familiar with the Fair Credit Reporting Act and how litigious that has been. It provides us some glimpse into what other privacy and types of litigation we're going to be seeing from plaintiffs, and I think the more important point to make in the context of this question, Chris, is the documents you're creating as you look at compliance and deal with the regulatory issues that Kim and I know you talk about become the exhibit that we have to deal with in litigation. And what I'll continue to remind people is you need to be thoughtful of that, especially when you're dealing with technology in your IT department, be

thoughtful now about what documents your business is creating and what they'll look like when it's displayed in front of a jury or a judge.

Chris Willis:

That's really interesting. On the data breach side, have there been any recent notable decisions from the courts that our readers would like to hear about?

Ron Raether:

Without question, and frankly, *Ramirez* is just another turn in the cycle of standing in damage and harm issues that we've been addressing in the data breach cases since I defended my first one in 2005. So, what we've seen in those cases is plaintiffs getting bogged down in the standing causation damage issue, and most of the cases resulting in either a quick low settlement or success on a motion to dismiss. Now, *Ramirez* created a brand new set of interesting circumstances for us. Do we want to end up in state court? If we succeed on *Ramirez* and we're out of federal court and we want to see where state courts have a more lenient standing requirement like California, do we want to see those cases in state court? Do we want to see 20 or 30 of them as opposed to one?

The other thing that we're seeing, with plaintiff's counsel starting to cross that standing damage threshold discovery, and ultimately, motions for class certification, which have been very rare in data breach cases. The most notable decision right now is Judge Grimm and what he decided in the *Marriott* case, and in that *Marriott* case, the issue was really ascertaining a class. How do you prove damages on a class-wide basis? And Grimm came up with a model that I think is questionable in my experience in defending class actions, which I'll sum up as we'll figure it out later, figure it out later. Marriott filed a rule 23 F petition, which for those who are not [inaudible 00:15:14] pro people, means that they went and sought appellate review in the middle of the case, and the Fourth Circuit took that appeal. So, it's going to be interesting to see what this Fourth Circuit does with these issues that Judge Grim primed up in the *Marriott* case.

Chris Willis:

Turning to the state law front, and you mentioned California, Ron, what's the status of litigation under the California Consumer Privacy Act? Are private plaintiffs beginning to bring claims under that act and how have they fared if they have?

Ron Raether:

They have been, and I'll take it a step aside for a moment and just talk about CCPA, especially at the financial institution. So, I'm sure, Chris and Kim, you've been involved in conversations with your clients about the exemption of entities that are regulated by the GLB, Gramm-Leach-Bliley. And then that moves into the conversation of do you have data in your institutions and your technology that are not regulated by GLB? So, we're really talking there about marketing, right, and some of the data that our financial institution clients are collecting that aren't NPI so it's not data that's regulated by Gramm-Leach-Bliley. And that really turns then to plaintiff's counsel are creative. They are testing the waters in terms of these privacy statutes and figuring out how they can make hay, and they're okay losing a few times here or there. And with respect to the CCPA, obviously, that statute has provision on data breach, and I'm not really talking about that at this point.

I'm more focused on what we anticipated, which was the use of the privacy requirements under the CCPA to argue an unfair deceptive trade practice claim. So, we've seen that arising in complaints. We've actually had one case that we're involved in where plaintiff's counsel tried to argue that the statutory damages provision, which is intended to only apply in the data breach context, extends to privacy violation. We were able to get the judge to grant a motion to dismiss saying, plaintiff, you're wrong. It is limited to data breach. But I wouldn't be surprised because that was one district court, we don't see that reemerge in other cases.

The UDAAP case, and then there's an invasion of privacy claim that's also still an issue in our case, create a really interesting set of dynamics for our clients because it really is talking about compliance, either as a business or a service provider, with the obligations that extend, whether it's CIPRA, CCPA, the Colorado, Utah, Connecticut, Virginia statutes. They can become a basis if you're not careful in terms of how you set up your compliance program.

But we're also seeing other theories. We're seeing claims being made under wiretap statutes, claims being made under the Video Privacy Protection Act, and this all circles back, Chris, to my point at the beginning, is that you may think you're exempt because it's GLB or DPPA or FCRA or it's publicly available information, those are some of the exemptions under a statutory claim, but you get caught if you're not being careful in how you're deploying technology. So, what am I tracking? What cookies am I keeping? Do I have a third-party marketing firm that I'm sharing that information with? Have I opted in what used to be Facebook Pixel, which is now Meta Pixel, or Google's equivalent in terms of tracking and marketing.

And we know, Chris, that those popups, those banner ads, they're putting aside the firm offer of credit issues. I know that we've engaged generally on those banner ads with financial institutions, providing general advertisements. In other words, we're not even crossing that firm offer of credit threshold, not bringing us into the FCRA, but needing to be thoughtful, does that create exposure under these other new privacy theories?

Chris Willis:

It sounds like there are a number of potential surprises there among the types of claims that are being asserted in privacy cases, Ron. Are there any others that are emerging that might be surprising to businesses that you'd like to tell our listeners about?

Ron Raether:

Thinking about marketing, looking at your technology, thinking about how your data, how you're acquiring data, who you're sharing that data with, it all goes back to the fair information practice principles which we know is the foundation for all these laws frankly, all the way back to the FCRA and the Privacy Act. Whether you're going through this exercise because you're obligated to do it under a statutory scheme or you're doing it as just part of good compliance, it's an exercise that will build the muscles that we need, both as a business, but going back to one of my other points, Chris, we have to be thoughtful about the documents that we're creating that are going to end up as exhibits in the cases that we're litigating, and care needs to be taken with respect to these issues.

Chris Willis:

That sounds like excellent advice. Thank you, Ron, and thank you, Kim also for being on today's podcast. The two of you have together delivered a really great update on everything that our listeners should be aware of from a privacy and data security standpoint, and I know that both of

you are going to continue to work very closely with our financial institution clients on those issues. So, I want to thank you for being on the podcast today, and of course, thank you to our audience for tuning in as well.

Don't forget, of course, to visit our blog, consumerfinancialserviceslawmonitor.com, and hit that subscribe button so that you can get all of our daily updates on what's going on in the consumer finance industry. And head on over to troutman.com and add yourself to our consumer financial services email list so that you can get access to our alerts and webinar invitations. And of course, stay tuned for a great new episode of this podcast every Thursday. Thank you all for listening.