Business Better (Season 4, Episode 3): Cyber Adviser – Financial Services 2024 Privacy and Cybersecurity Preview

Speakers: Greg Szewczyk and Sarah Dannecker

Steve Burkhart:

Welcome to Business Better, a podcast designed to help businesses navigate the new normal. I'm your host, Steve Burkhart. After a long career at global consumer products company BIC, where I served as Vice President of Administration, General Counsel and Secretary, I'm now special counsel in the litigation department at Ballard Spahr, a law firm with clients across industries and throughout the country.

This episode is part of our CyberAdviser series where we discuss emerging issues in the world of privacy and data security. The privacy and cybersecurity landscape is evolving in the financial sector from more specific data security reporting requirements to potential data subject rights, and the use of artificial intelligence.

Today, our lawyers will highlight key developments and provide practical insights on how to stay ahead of the regulatory of litigation and hacker threats. Participating in this discussion are my Ballard Spahr colleagues, Greg Szewczyk, leader of the Privacy and Data Security Group, and Sarah Dannecker, an Associate in the Privacy and Data Security Group. So now let's turn the episode over to Greg.

Greg Szewczyk:

Hey everybody, and welcome to our first webcast of our monthly series of 2024, which is the Financial Services 2024 Privacy and Cybersecurity Preview. Before we get started, I just want to make sure everybody's aware of a couple of public resources for both privacy, cybersecurity and consumer finance blogging and podcasts. We've got the Consumer Finance Monitor, which is an ABA award-winning blog. We have the CyberAdviser award-winning blog about all things privacy and data security.

And then we also have the Consumer Finance Monitor podcast that's available on Apple iTunes, Google Play, Spotify, and your favorite podcast apps. So you know who is talking at you today. My name is Greg Szewczyk. I'm a partner in the privacy and data security group here at Ballard Spahr. And joining me is Sarah Dannecker, who is an attorney in our Minneapolis office who specializes in not just privacy and cybersecurity, but also various different financial services and banking matters.

So I've got the agenda up on the screen today. One thing I want to mention is there is a lot going on in this area. There's a lot going on in each of the things we're going to talk about. In certain of these things we have done 60 and 90 minute podcasts on just the topic. The point of these webcasts is not going to be necessarily to do a deep dive on any of them, but instead just to make sure that we're highlighting potential issues.

And we're going to keep this short, we're going to keep it usable, but if there's ever any kind of stuff, questions on specifics or anybody wants to dig down a little deeper, some of these you can find more information, longer webinars on those blogs and podcasts that we mentioned. And you could also always reach out to me or Sarah and we can direct you to those resources or talk about what you would need specifically. So what we're going to be kicking off with today is the FTC safeguards rule and data breach reporting. Then we're going to move down to the SEC's new cyber incident reporting. We're going to talk about the CFPBs proposed rule on personal financial data rights.

We're going to talk about the New York DFS's updates to the cyber security requirements. And we're going to talk a little bit about what's going on on the AI front, which is likely going to be dated by tomorrow because the regulatory landscape in that field is changing so quickly. But again, we're going to keep it at somewhat of a high level and try to give some practical takeaways from this. So with that, I'm going to turn it over to Sarah to get us started with the FTC safeguards rule.

Sarah Dannecker:

Thanks, Greg. Appreciate it. All right, so I'm going to chat today as Greg mentioned, about the amendment to the FTC safeguards rule for data breach reporting. So on October 23rd, the FTC announced that it had finalized the amendments that it proposed back in 2021, which will now see financial institutions required to report certain data breaches.

So for a little bit of background, for those of you watching, some of you may recall in 2003 that the FTC issued the standards for safeguarding customer information, which is known colloquially as the safeguards rule, to kind of ensure that financial institutions or entities that are significantly engaged in financial activities maintained certain safeguards to protect customer information.

And this rule was amended in 2021 to implement certain changes to kind of keep pace with changes in technology, to strengthen data security requirements for covered entities, and then to provide some more concrete guidance for businesses. And then as part of those 2021 amendments, the FTC sought comments on a proposal that would require financial institutions to report certain data breaches and other security events to the FTC.

If you want to go to the next slide. So effective as of May 13th, 2024, financial institutions must now notify the FTC no later than 30 days after discovery of a notification event involving at least 500 consumers. And a notification event is defined as the acquisition of unencrypted customer information without that customer's authorization. So a notification is going to be made electronically through a form that would be available on the FTCs website.

Must include information regarding the type of information involved, the date of the event or the date range of the event, and kind of a general description of it. And so this is in addition to any state law requirements for breach notification. So this is just another entity that's going to need to be notified in the event that this 500 consumer threshold is triggered, which is again, in line with a lot of state law breach data breach requirements for notifying the state's attorney general, is that 500 consumer threshold. So just putting that on people's radars.

If we want to go into the next slide. Next we have the SEC cyber incident reporting rules. So on July 26th, 2023, the SEC dropped its new rule requiring public companies to disclose material cybersecurity incidences in what I would call real time and then to annually disclose material information about their cybersecurity risk management, their strategies, their governance procedures, things like that. And then foreign private issuers are going to have comparable disclosure requirements.

So this became effective as of September 5th, 2023, and companies are going to now have to disclose any material cybersecurity incident generally within four days of the date that they determined that the incident was material. So this is done in a periodic report known as an 8-K. Companies need to describe the nature of the scope, the timing of the incident, and also the material impact to the company. And then in terms of annual disclosures, those are done on the form 10-K reports.

And companies now need to disclose their processes for managing material risks from cybersecurity threats. So companies need to start assessing kind of how cybersecurity risks do or could have an impact on the company, including effects from any previous incidences. Disclosures regarding oversight. Board oversight of cybersecurity risks are now also required. So things to keep in mind if board members or executive officers do not have significant cybersecurity expertise. This would be noted in these disclosures as well.

And we're already seeing companies preparing for these because the fiscal year, December 31st, 2023 form 10-Ks are now being filed beginning of this year. If we want to go to the next slide. Interestingly enough, there may be some unintended consequences of the SEC rule, which I just wanted to talk briefly about because I found it pretty interesting. But in November of last year, there was an article about a ransomware group that had published screenshots of an SEC complaint formed that the group itself had filled out against its own victim, MeridianLink.

Whether the complaint form was actually submitted or not was at least at the time the article was written unknown. The SEC had not confirmed. But the group claimed that it had orchestrated a significant data breach against MeridianLink. And MeridianLink is a company that provides digital lending and account opening services for financial institutions. And the group claimed that as of the date, at least the date that the article had come out, MeridianLink had not reported this incident in a form 8-K.

MeridianLink later came out with a statement saying that the incident was not material and therefore was not required to be disclosed under the rules. But regardless, at least some damage may have already been done just through the publication of the

article and the sheer audacity of the act, I guess, and may have been the ransomware group's purpose at the end of the day to kind of further future ransomware negotiations. So who knows, it's just an interesting potential unintended consequence. So I'll turn it over to Greg now.

Greg Szewczyk:

Thanks, Sarah. So I'm going to hit quickly the CFPBs personal financial data rights rule or proposed rule 1033. This is one of those where we have done a full hour long webinar last year. If anybody's interested in really drilling down into the specifics of this proposed rule, you should go check out that webinar that is publicly available through Ballard Spahr or reach out to one of us and we can get you in touch with it.

But at the 30,000-foot level, the proposed rule provides new rights and imposes new obligations related to certain types of consumer financial data, and that includes a right of access for both consumers and third parties. And there's a right of data portability component in that. So as the CFPB has said, that data portability component is designed to try to decrease stickiness and promote competition. Data portability is a component of most privacy laws, but it's one that usually does not really get front and center attention in the compliance mindset.

But in this context, it is actually pretty important because it would allow consumers who have accounts with certain types of financial institutions, an easier ability to move to a competitor. It also requires this type of sharing to be done through interfaces that is designed to move the industry away from screen scraping. So that's another pretty big shakeup that would be coming down if this proposed rule is finalized.

The rule would also impose what would be very significant limits on how third parties can use data with the exact impact still somewhat up in the air. And it would expand the scope of data security regulations, especially the GLBA safeguards rule that Sarah was just talking about, which for those familiar with the financial services world, know was updated in a different way earlier that went into effect in June of 2023.

That really put a lot more specific requirements on what kind of security measures need to be in place and how they need to be documented. So if proposed rule 1033 is adopted in a similar form to what it is, it's going to have some pretty significant operational impacts for a lot of companies on several fronts. The first thing to address with that is who the rule would actually apply to. And the good news is that the rule would only apply in a limited context at first.

The rule would govern two categories of covered persons, data providers, and third parties. Data providers is defined to mean an institution under regulation E, card issuers under reg Z or any person that controls or possesses information concerning a covered consumer financial product or service obtained from that person. So we're talking about entities like banks, credit unions, and other providers of checking, savings and credit card accounts and other various kinds of payment accounts and products.

The third category encompasses a wide range of non-financial institutions like digital wallets, which is specifically discussed in the CFPB's examples. The proposed rule would have a limited exception for depository institutions that do not have a consumer interface as it's currently structured. So the good news is that the current proposed rules does not apply to the full scope of financial products and services it could like mortgage, auto or student loan payment accounts.

The bad news is that the CFPB has already stated that it would intend to implement the rule to those other covered entities through supplemental rulemaking. So even if your entity's not going to be within the scope of 1033 immediately, it still could be and there's a need to keep on top of how it would apply should the rulemaking ultimately expand the scope. Third party's define to mean any person or entity that is not the consumer about whom the covered data pertains or the data provider that controls or possesses the consumer's covered data.

So a third party could be another financial institution, that could be a data provider in its own right, but it would also include FinTechs and data aggregators. And the proposed rule has some special rules for data aggregators, which would be defined as a way that retained by and provides services to the authorized third party to enable access to covered data.

So like I said on the last slide, there's too much to unpack to go through it for this type of a quick webcast or podcast, but one of the biggest takeaways is that these third parties, a lot of FinTechs, are going to have to be subject to the updated safeguards rule. That's been an issue about which there has been some confusion, but now when 1033 goes into place, that ambiguity just has, it goes away.

It's going to be a big change for a lot of FinTechs. And there's also going to be some serious limitations on the way data can be used without express consent from consumers. So if you are in this field, this is very much something that you need to be paying attention to. Another area that everyone needs to be paying attention to is the New York DFS's cybersecurity regulation that was updated last year. Those changes are already in effect for the most part.

Again, this is one where we could spend a whole hour talking about them. But to kind of hit the high level, one of the changes is that there are new classes of companies under the New York DFS rule. A class A company consists of a covered entity with at least 20 million in gross annual revenue in each of the last two fiscal years from all of its business operations that either employ over 2000 employees averaged over the last two years, or has over a billion in gross revenue in each of the last two years from all of its business operations.

So part of what we're seeing here is an attempt to add additional requirements to larger entities and the business operations need to be considered the aggregate whole of the entity, not just one specific line of business. If you are a class A company, there are additional requirements under the New York DFS's amendments. These range from heightened risk assessments to other issues. But for all companies, there are also some additional requirements.

There are expanded incident reporting requirements. There are additional specific security requirements. Some of these are specific like the expanded use of multifactor authentication whenever anybody is accessing systems. That is largely in line with what we see in the GLBA's updated safeguards rule that we were just mentioning. There's also the expansion of the trend that we have seen to require more and more written policies, not just to have certain policies in place.

And as people who are familiar with the New York DFS know there needs to be a certification on an annual basis of compliance, which means that there will be a certification that you do have these written policies in place. So it's an important change and it's something that needs to be, even if the technical procedures are already in place, companies need to make sure that they're documenting this in the correct way.

The last thing we're going to hit quickly is AI and cyber policies. It seems like there's hardly a week that goes by that we don't have a new announcement about some kind of AI regulatory effort or legislative effort. What I have up on the screen here is just a few in the financial services world. We've seen the CFPB, the DOJ and the FTC and the EEOC put out a joint statement about how AI could result in unfair and discriminatory effects and that these fall under the already existing authorities of these agencies.

The CFPB last fall issued some other guidance on credit denials by lenders using AI. The FTC has said that it is going to regulate specifically marketing about AI capabilities. The White House executive order from last October is going to touch the financial services world. And then we also, we are starting out the state legislative cycle right now, and it's highly likely that we are going to see AI specific bills being introduced and some of them being passed.

It's yet to be seen how or if those will have any carve outs for the financial services world, but it's likely that those are going to impact a lot of financial services or FinTechs along the way. So it's an area where you just kind of need to stay on top of it. What we are seeing as far as four concepts within all of these regulatory frameworks, it all kind of leads us to a multi-pronged approach of not just tracking the regulations, which you obviously need to do, but having a system set up where there's transparency, there's risk assessments, there's accountability, and there's corporate governance.

And so in large ways, this has followed what we've seen in the privacy and cybersecurity world more generally, but we're starting to implement that on the AI basis. So as some practical steps that can be taken right now, not just track regulation, but start developing AI governance programs. We've seen a lot of clients leverage their existing privacy and data security programs for this. These programs should have periodic risk assessments.

They should assign management responsibilities, they should ensure board reporting, really the same type of criteria that we have seen required under the, some of these new laws that we were just talking about earlier. There's also a big focus on vendor management. A lot of companies don't necessarily develop their own AI, but they're using third party products that do leverage AI. There are state privacy laws that require specific types of risk assessments internally when doing that.

There's proposed regulations under this for the CCPA that would have some pretty specific requirements for what would need to be in those. And then this could also come into context with a cross border transfer depending on how the AI system's structured. So although the actual contractual language may not necessarily change a lot, there is a very large and growing need to continue to drill down what type of data is being used by that vendor and how it's being used.

And that's just something that should already be occurring, but needs to occur more and more. And what we're seeing in these draft regulations and what we're hearing about proposal legislation is that this is going to be a big focus. So it's something that should be started to be worked into the vendor management and contracting process now, to the extent it's not. With that, I'll turn it over to Sarah to give us some final thoughts.

Sarah Dannecker:

All right. Thank you. All right. I'll just kind of close it out with just some thoughts, perhaps some predictions for the remainder of 2024 and beyond. If we want to go to the next slide. At the state level, we're likely to see movement on the set of proposed revisions to the California Consumer Privacy Act regulations that the CPPA issued in December of last year.

And while maybe not entirely germane to financial institutions, because most financial institutions are going to be exempt from the CCPA under the GLBA, it's kind of important to just have an awareness of what's going on, at least at the state level, particularly with the CCPA. And these amendments were released in connection with the CPPA.

That's the agency that's tasked with enforcing the regulations with their December 8th board meeting and include revisions to things like sensitive personal information categories, changes to the monetary threshold or applicability, and binds included some modifications to certain consumer rights and then opt out preference signals, more specifically bringing back the requirement that businesses need to display whether they've processed an opt-out preference signal. On the federal level, maybe some potential for movement on a harmonized cybersecurity regulation.

So the Biden administration through the Office of the National Cyber Director released an RFI in July of last year, soliciting comments on how to potentially harmonize cybersecurity regulations in the wake of these continuing cybersecurity proposals and expectations that are starting to kind of create this complex compliance burden on organizations that span multiple sectors, many of which are already subject to cyber incident reporting and regulatory obligations.

So potential there for something. And then finally, as Greg touched on, I think again, we're only going to continue to see issues pop up surrounding AI, both from a regulatory scrutiny perspective and then from the consumer protection side. I know from conversations that I've had with colleagues that work in-house, it's top of mind for developing AI models using AI. It's not something that's going to be going away. So all this remains to be seen though. So unless Greg, do you have any final thoughts?

Greg Szewczyk:

No, just thanks everybody for tuning in. We're going to be kicking these back up and doing, trying to do this on a monthly basis. You can always reach out to me, you can reach out to Sarah. We're always happy to talk about anything and see how we can help anyone. So thank you all for tuning in, and we'll see you next month.

Steve Burkhart:

Thanks again to Greg Szewczyk and Sarah Dannecker. Make sure to visit our website, www.ballardspahr.com, where you can find the latest news and guidance from our attorneys. Subscribe to the show in Apple Podcasts, Google Play, Spotify, or your favorite podcast platform. If you have any questions or suggestions for the show, please email podcast@ballardspahr.com. Stay tuned for a new episode coming soon. Thank you for listening.