THE CONSUMER FINANCE PODCAST: THE NYDFS UPDATES ITS STRINGENT CYBERSECURITY REGULATIONS. IS THIS A BELLWETHER OF COMING INDUSTRY CHANGE?

HOST: CHRIS WILLIS
GUEST: KIM PHAN
DATE AIRED: NOVEMBER 16, 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. I'm glad you've joined me for today's discussion, which is going to be all about the New York Department of Financial Services updates to its cybersecurity regulations, which is an issue of great importance to our community. But before we jump into that topic, let me remind you to visit and subscribe to our blogs, troutmanpepperfinancialservices.com and consumerfinancialserviceslawmonitor.com. Don't forget about our other podcasts because we have lots of them. We have FCRA Focus, which is all about credit reporting, we have The Crypto Exchange all about cryptocurrency issues, we have Unauthorized Access, which is our privacy and data security podcast, and our newest podcast Payments Pros, which is all about of course the payments industry. They're all available on all the popular podcast platforms, just like this one is.

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. If you enjoy listening to and reading our content, one of the great ways to get at it is our new mobile app. You can find it for both iOS and Android in your app store under Troutman Pepper. It has all of our blogs, all of our podcasts, a great nifty directory feature, and even a calendar that tells you which conferences we'll be attending next. If you'd like to check that out, just go ahead and download it from your app store.

Now, as I said, we're going to be talking today about updates by the New York Department of Financial Services to its cybersecurity regulations. This seems like a particularly pivotal development for us because the New York DFS has been one of the most active regulators in terms of cybersecurity regulation. I'm really lucky to be joined by my partner, Kim Phan, who's from our privacy and cyber group to talk about what New York DFS has done here. Kim, welcome to the podcast and thanks for being on today.

Kim Phan:

Thank you for having me, Chris. I'm always thrilled to come speak to you about the latest developments.

Chris Willis:

Well, you're a great guest to the podcast and so I appreciate you continuing to be on whenever these interesting things happen in the world of privacy and data security, which is of such importance to financial services companies. The New York DFS is sort of at it again, essentially being the defacto national leader in terms of regulation in this area. Can you give the audience some background on what DFS has done with regard to updating its cybersecurity regulation?

Kim Phan:

Thanks, Chris. This is a major development because New York DFS has been... Let's say they're the furthest forward thinking in this area of any regulator in the country right now. When they first promulgated their cybersecurity regulation back in 2017, it was the strictest regime imposed by pretty much any state in the country for any industry, especially for the financial industry. When they announced updates last year in June 2022, I think the entire industry sort of was shaking in their boots.

Their justification for the need to update the regulations, which, again, are by far the strictest in the country, was because data breaches are still happening so obviously they didn't go far enough. They've decided to go even farther and update and increase the expectations of licensed entities in New York. They released their draft in November of 2022, the revised draft, which actually took into account some changes in response to public comment which I was surprised by. In the past, they have not necessarily made changes that were directly responsive to concerns by the industry, but they did make a number of edits and they released the revised draft in June earlier this year, which was finalized on November 1st.

Chris Willis:

Got it. Did these latest amendments pull any more or fewer companies under the scope of the regulation?

Kim Phan:

Interestingly, it's a little bit of both. There are entities that have now been defined by New York DFS as class A companies, so while these companies would have been subject before to the cybersecurity regulation, they now have an entirely new set of obligations under the new updates for companies that have $20 million in gross annual revenue in New York and one of these other two factors, so $20 million in gross annual revenue in New York plus over 2000 employees or $20 million in annual gross revenue in New York plus $1 billion of annual gross revenue anywhere in the world, so worldwide. If you're the biggest of the big, this will apply to you regardless if you're operating in New York.

Now, they have also expanded some of the small business exemptions. Here's where I said there will be some entities that will drop out. For the employee exemption, they've expanded it to include not just entities that have less than 10 employees but now have grown that exemption to less than 20 employees. However, that includes not just direct employees but also the employees of affiliates as well as independent contractors. The small business revenue threshold has also been increased from 5 million to $7 million annual gross revenue, but that now will include revenue anywhere in the world as well as for New York affiliates.

The total assets small business exemption has also been increased from $10 million in total assets to $15 million, but keep in mind to qualify for any of these exemptions there is a new process laid down in the rules with regard to how to apply. There is very distinct and specific information that has to be provided for New York DFS to consider in granting an exemption, and the entity that is seeking the exemption must continue to comply until they get a written determination of an exemption from the New York DFS superintendent.

Chris Willis:

Okay. We know that there's been some in and out with respect to who's covered by the cybersecurity regulation. I had noted that there was also some new obligations that are being imposed on the governing bodies of companies. Can you tell the audience a little bit about that?

Kim Phan:

Sure. There's this expectation now that there needs to be more governance, more accountability from the upper echelons of companies to be overseeing and taking responsibility for the cybersecurity maturity of their organization, so there's an expectation now that senior governing bodies must now exercise oversight. That oversight requires, according to New York DFS, that they have sufficient understanding of cybersecurity, otherwise they can't properly oversee cybersecurity programs. Now, to the extent that's necessary, if they don't have on the board someone who happens to be a technical expert in this area, they can use advisors and there's an expectation they bring in the expertise needed to help explain some of these cybersecurity issues if they themselves don't have the internal knowledge.

They have to receive regular reports on cybersecurity matters at their governing meetings, not just the annual report that was already required to be delivered to them by their CISO, their chief information security officer, and they're now responsible for ensuring that the CISO and others within their security teams have sufficient resources, whether or not that's FTE, full-time employees, or whether or not that's funding to purchase the latest widget or solution that is expected, and they have to approve the company's cybersecurity policy on an annual basis. Again, you can't just develop a policy and set it and forget it. They have to actively be reviewing this on an annual basis and approving it for their organization.

Chris Willis:

Well, you mentioned policies there, and you and I participate in a lot of New York DFS examinations of companies and assist companies with those exams and it is incredible the degree of attention that the examiners pay to the exact wording of policies and procedures related to cybersecurity. Is there anything in this new updated regulation that will require any policy updates by covered companies?

Kim Phan:

There will. There's an expectation that policies be expanded to cover a whole variety of new topical areas, specifically things such as data retention and end of life management. When you're done with data, what do you do with it? How do you dispose of it? There's a new concern around remote access controls as more and more folks are working remotely rather than being in the office. There's a lot of concern about the security risks that may be presented by that. The need for monitoring of systems and networks, the need for training, and specifically they call out training in response to social engineering threats, so the idea that someone might call in and pretend to be a consumer in order to seek additional information to engage in some sort of malicious activity, presumably identity theft or other types of fraud, expanded requirements with regard to incident notification, as well as a more robust program for vulnerability management.

Chris Willis:

Okay. That's a lot. Let me pick up on the last thing that you just mentioned about vulnerability management. What specifically will companies need to do to update their vulnerability management protocols under this new regulation?

Kim Phan:

Sure. When we say vulnerabilities, we're talking about vulnerabilities to your data, risks, threats. Already companies were required to do penetration testing, the idea that you're going to test your security controls to see whether or not they're working, but the New York DFS has added that those tests have to occur from both inside and outside your system's boundaries, specifically addressing the idea that they're not only external threat actors that are trying to get this data but you could have insider threats, people who are trying to access your system without authorization for whatever purpose even though they are already an existing employee.

Automated scans have to be supplemented by manual scans, manual reviews by actual security team members. If your systems are not able to be scanned systematically or automatically through solutions or other tools, that's going to be a huge investment of time and resources, manpower to achieve that, as well as a whole host of new monitoring that they're expecting, for example filtering web traffic, monitoring emails to block malicious content. Class A companies, as I mentioned, the largest of the large will have additional obligations such as implementing endpoint detection solutions for finding and identifying anomalous activity as well as a centralized logging solution to alert the security team in the event of some sort of security event. To the extent that their vulnerability detection processes identify any vulnerabilities, there's a clear expectation now in the rules that not only do you have to know that these vulnerabilities exist, you have to now remediate them not just accept that that risk exists.

Chris Willis:

Got it. I've often heard folks from the New York DFS talk about the virtues of multifactor authentication. Is there anything about that in the new cybersecurity regulation?

Kim Phan:

Multifactor authentication already existed in the regulation. I think they just wanted to clarify that it is a clear expectation in basically every scenario in which access to the system is occurring. They gave three specific examples that clarify, "Here are some additional scenarios that if you were not already deploying multifactor authentication in these areas that you should be doing so." Any sort of remote access to the company systems, which I mentioned, there's a big concern now about remote access and remote employees, remote access to company applications that are hosted on the cloud, so maybe you're not directly going into the company network but you're accessing some sort of application hosted on a cloud platform as well as privileged accounts. There's a lot of focus in the new regs about privileged accounts. These are those accounts for those individuals, and this should be a small number of folks, who essentially have the keys to the kingdom. This is the CISO who has credentials that can essentially allow him or her to access any data or system within the organization, so a lot of controls around that.

In addition to multifactor authentication, there are a bunch of new other just general access controls, things like having limited numbers of privileged accounts, annually reviewing who has access to what accounts, so maybe someone either gets promoted or demoted or moves laterally within the organization, making sure that their access settings are reflective of their existing job responsibilities, as

well as, this is new, having a written password policy. I think most of us are aware that there are technical controls around passwords, it has to be of a minimum length with certain complexity. Now New York DFS is expecting that be written down in a specific way so that companies have that, and that class A companies specifically, again the largest of the large, have to have technical controls that block the most commonly used passwords, things like password as your password.

Chris Willis:

For those highly original employees who like to use those.

Kim Phan:

Correct.

Chris Willis:

What about data inventories, Kim? That seems like something that also might be called for under the new regulation.

Kim Phan:

Yeah. Data inventories is a growing concept that we see a lot. It's not expressly called out, say, in California or by the FTC per se and not even by New York DFS. New York DFS addresses the idea that companies really need to inventory what data they have and where it's stored by imposing obligations with regard to asset management. New York DFS is expecting its covered entities to now track data assets. Who's the owner of those assets? Where are those assets located within the organization? What's the classification about that data? Is it sensitive? Is it confidential? Is it public? When should that data expire, meaning when should companies be getting rid of it, as well as how important it would be for a company to recover that data if there was some sort of incident like a ransomware attack?

Chris Willis:

Got it. Speaking of an incident, what will companies need to do in connection with the new version of the regulation about their data breach response plans?

Kim Phan:

Data breach is an issue that they spend quite a bit of time in the new updates making sure that companies' obligations in response to different types of security events are incredibly clear. For incident response plans, they're now expecting that companies incorporate into those plans how to engage in business continuity and disaster recovery procedures, how to respond specifically to ransomware, they talk about identifying essential data and personnel, what the DOJ has characterized in the past as the crown jewels of an organization, what is so critical that it has to be protected more than other data or has to be recovered more quickly than other data.

They're expecting that companies deploy a communication plan about how to communicate with not just other employees, but counterparties that may be relevant in an incident, regulators, service providers, disaster recovery specialists, senior governing bodies, specifically calling out the need to have backups, copies of all data. That data has to be backed up sufficiently frequently to protect the organization and its operations and any stored copies have to be stored offsite. Now, there's some cost

that is associated with that type of requirement. Then after an incident, the New York DFS is now saying that the entities now have to do some root cause analysis of what led to that incident, how they're going to update their plans, and then the incident response plan has to be distributed to all employees.

We've actually worked with companies who have encountered ransomware attacks, and their plan was stored electronically on their system and no one could access it so having a paper copy is one of those things that just makes good sense but now New York DFS is expecting. They also want companies to test these plans, typically through what we characterize as tabletop exercises, you get all your key stakeholders together and you run through a scenario in which you are simulating an attack, but they also want to see technical testing as well, the ability to restore data from your backups, how quickly can you get those materials from offsite, how quickly can you upload them and restore customer facing financial products and services.

The notification to the New York DFS within 72 hours, that was a preexisting requirement, but now New York DFS has said that there will be a web form that companies can use to provide that notice. But in addition to the initial notification, they are very clear and they added into the regs that there is an ongoing obligation to update New York DFS as you continue your investigation. As you learn more facts about what happened in an incident, you've got to let the New York DFS know, especially if you are in a position where you have to make a ransom payment. New York DFS characterizes that as an extortion payment, but it's the same, right? You get a ransomware attack, someone's trying to extort money from you, and you have to pay. New York DFS not only wants a notification within 24 hours of the payment, but also within 30 days following the payment they want an additional explanation. Why did you pay? What alternatives did you consider before you made that payment, and how did you comply with things like OFAC and other BSA/AML obligations with regard to making that payment?

Chris Willis:

I didn't know about the OFAC piece of it. That's very interesting, actually. I mean, how would a company paying a ransom even know necessarily? Are they going to get a social security number from who they're paying?

Kim Phan:

There are some vendors and some other tools that have attempted to identify well-known hacking organizations. These guys are starting to get famous because take they'll down the largest companies they can to make a name for themselves, and there are entities that are tracking some of the money flow to those entities to see whether or not it's associated with any of the entities that appear on the OFAC list.

Chris Willis:

Okay, got it. Now one of the things that I've always found very notable about New York's regulations relating to this is the annual certification requirement that covered companies don't just have to comply with the rules, they have to file a certification with New York DFS saying, "I have complied with all your rules this year." Has there been anything that's changed about that certification requirement in the new regulations?

Kim Phan:

I think that New York DFS got wise to the company strategy of having some low level whoever sign these certifications, someone who doesn't actually have oversight over the program, so the new certification requirement is that the certification must be signed by the highest ranking executive within the organization, typically the CEO, as well as the CISO. These are folks that the New York DFS I think will be hoping to bring personal liability against in the event of some sort of issue. There's also actually a new alternative that I think is actually useful. The certification previously was very all or nothing, we were either 100% compliant or we don't certify at all, right?

Chris Willis:

Right.

Kim Phan:

There was no wiggle room on that. The New York DFS now has an alternative, a written acknowledgement of non-compliance where you can basically say, "We're certifying compliance in all of these areas except for these few." They have to identify specifically what those areas are and then also propose a remediation timeline for when the company expects to be able to comply in those areas, but, again, that also needs to be signed not just generally, it doesn't have to be just generally submitted, it has to be the CEO or the CISO. Again, I think the New York DFS is looking toward individual liability.

Chris Willis:

Speaking of liability, that sort of brings us to the subject of enforcement. How do you think the New York DFS is going to go about enforcing the new requirements that you've been spending the last 20 minutes telling the audience about?

Kim Phan:

Sure. New York DFS has clarified in these new updates that any single act that is prohibited or otherwise leads to non-compliance is potentially a trigger for compliance and liability. If you fail to prevent some sort of unauthorized access, that's given as an example of a potential compliance failure. If there is any material failure to comply in any 24-hour period, that potentially leads to a daily penalty by the New York DFS. So very clear New York DFS has a strong intent to bring penalties, whether or not that's individual liability, company-wide liability, whether or not that's a strict liability regime, whether or not penalties will be calculated on a daily basis. All of these are things that if I was a company operating in New York DFS jurisdiction, I would have some concern about.

But New York DFS I think was aware that this might be something that would be scary, and so they listed a number of factors that they will consider in assessing penalties, things like whether or not the company has cooperated with New York DFS, whether or not they've acted in good faith, whether or not it was an unintentional or inadvertent failure, a history of previous failures, whether or not there was any harm to consumers, whether or not a company has been good about sending out accurate and timely updates and notifications to not just New York DFS but to customers. There's a number of factors that New York DFS says they'll consider in addition to the actual violation itself when assessing penalties.

Chris Willis:

Got it. There's clearly a whole lot going on in terms of these new updates to the cybersecurity regulation, a lot for companies to take into account, but good thing is that we have the expertise to offer them through you and your colleagues of being able to adapt to these new changes. Kim, thanks a lot for being on the podcast today, and of course thanks to our audience for listening in as well. Don't forget to visit and subscribe to our blogs, troutmanpepperfinancialservices.com and consumerfinancialserviceslawmonitor.com.

While you're at it, why not head over to troutman.com and add yourself to our Consumer Financial Services email list? That way we can send you copies of the alerts that we send out as well as invitations to our industry-only webinars. And of course check out our great mobile app. It has all of our thought leadership in one very convenient place. You can get it on either the iOS or Android app store under Troutman Pepper. Finally, stay tuned for a great new episode of this podcast every Thursday afternoon. Thank you all for listening.