Consumer Finance Monitor (Season 4, Episode 49): The Federal Trade Commission's Updated Gramm-Leach-Bliley Act Safeguards Rule – What You Need to Know

Speakers: Alan Kaplinsky, Kim Phan, and Doris Yuen

Alan Kaplinsky:

Welcome to Consumer Finance Monitor podcasts, where we explore important developments in the world of consumer financial services. I'm Alan Kaplinsky, senior counsel at Ballard Spahr, former chair for many years of the Consumer Financial Services Group at Ballard Spahr. I'm very pleased that you've downloaded this podcast show that we're going to be presenting today. The podcast show is based substantially on a topic that we covered during a webcast, not too long ago, but I thought it was a sufficiently important topic, and I know many of you did not have the opportunity to attend that particular webcast that is in the privacy and data security area of Consumer Financial Services.

Alan Kaplinsky:

So, let me just give all our listeners a little bit of introduction on the topic, and then I'll introduce our speakers, and then turn it over to them to carry the ball. So, what's prompting this podcast today is that the Federal Trade Commission, not too long ago, finalized updated rules, implementing the Gramm-Leach-Bliley standards for safeguarding customer information. Going forward very often, we'll refer to Gramm-Leach-Bliley as simply GLBA. What we're going to be talking about today are some updated rules that are implementing the GLB standards for safeguarding customer information.

Alan Kaplinsky:

The prior approach that was taken under the safeguard's rule allowed financial institutions, the flexibility to develop a written information security program that was appropriate to a company size, the nature of its activities and the sensitivity of customer information. In today's podcast show, we will discuss the new approach under the updated GLBA safeguards rule, which lays out prescriptive requirements in the following five areas. One, specific aspects of an overall information security program. Two, accountability by boards of directors. Three, exemptions for limited collection of personal information, four, in expanded definition of what constitutes a financial institution subject to the rules, and five, newly incorporated definitions for the GLBA privacy rule.

Alan Kaplinsky:

So, let me now introduce our presenters today on our podcast show. First, I want to introduce Kim Phan. Kim is a partner in our Ballard Spahr's D.C. office, who counts those clients on federal and state privacy and data security law and regulations, with a particular focus on consumer finance, but not exclusively consumer finance. Her work in this area encompasses strategic planning and guidance for companies to incorporate privacy and data security considerations through our product development, marketing and implementation.

Alan Kaplinsky:

Our second participant today is Doris Yuen. Doris is an associate in our Los Angeles office who focuses like Kim, on privacy and data security matters. She's counseled banking and non-banking institutions on financial services regulatory compliance matters and provides support for a government investigations. Prior to joining Ballard Spahr, Doris served as a legal intern at the Securities and Exchange Commission's office of international affairs, and Doris also spent time at the Consumer Financial Protection Bureau's office of fair lending and equal opportunity.

Alan Kaplinsky:

So, with that introduction, I'm now going to turn the program over to Doris, and I'm going to back away from the program today to let Doris and Kim really carry the ball. They are the true experts in this area. So, Doris, take it away.

Doris Yuen:

Thanks, Alan. I'm very excited to be talking with you all today about the FTCs amendments to safeguards role. I know many of our audience members today are probably busy wondering how the updates will affect their information security programs. So we'll just dive right in. First, I'll provide a bit of background to the Gramm-Leach-Bliley Act, AKA the GLBA and the FTCs safeguards rule. So the GLBA is a federal law enacted in 1999, and it provides a framework for regulating the privacy and data security practices of financial institutions.

Doris Yuen:

The FTC promulgated both a privacy rule and a safeguards rule under the GLBA, and the privacy rule went in effect in 2000, and it generally requires financial institutions under the FTCs jurisdiction to disclose their information sharing practices and allow customers to opt out of certain sharing with third parties. The safeguards rule, which we'll be focusing on today, went into effect in 2003, and it requires financial institutions to have a comprehensive information security program.

Doris Yuen:

So in the approximately two decades, since the safeguards rule was issued, the information security world has changed quite dramatically. Nowadays computer networks touch upon pretty much every aspect of daily life, and the number of frequency of data breaches and cyber tasks just keep going up. So the FTC felt that the safeguards rule may have been due for an update, especially since financial institutions can handle very sensitive customer information, such as social security numbers and account information.

Doris Yuen:

So in 2016, the FTC solicited comments on the safeguards rule as part of its periodic review of its rules and guides. In 2019, the FTC published its notice of proposed rule making to amend the safeguards rule to include more detailed requirements for the information security program. The amendments were based primarily on the cybersecurity regulations issued by the New York Department of Financial Service, and the insurance data security model law that was issued by the National Association of Insurance Commissioners.

Doris Yuen:

And in 2020, the FTC hosted a virtual workshop to further solicit public input on the safeguards rule. And then on October 27th, the FTC announced the final rule to amend the safeguards rule. The vote for the amendments was a three, two split with the three Democratic commissioners voting in favor of the amendments and the two Republican commissioners voting against. As of now, the final rule still hasn't been published in the federal register yet, so the old rule is still in effect.

Doris Yuen:

But currently the safeguards rule requires that financial institutions have a comprehensive information security program that is written, and that contains administrative, technical and physical safeguards appropriate to the size and complexity of the financial institution, the nature of its activities and the sensitivity of the customer information that's maintaining. The safeguards must also be reasonably designed to ensure the security and the confidentiality of customer information.

Doris Yuen:

It should also protect against any anticipated threats or hazards to the security or integrity of that information, and it should also protect against unauthorized access to, or use of such information that could result in substantial harm or inconvenience to any customer. Now, the new rule generally still requires that, but it also dictates that the information security program have

very specific elements to it. Whereas before the rule provided more general guidance that generally gave financial institutions flexibility to make their own decisions about a specific controls to put into place.

Doris Yuen:

Now, although many financial institutions may already have some of these new elements from the new rule as part of their existing information security programs, the FTC felt that there was value in making such requirements explicit, such as the development of a written incident response plan, even though certain state laws might already require such institutions to have such elements in place. So we'll talk now about the new requirements of the updated rule.

Doris Yuen:

One new requirement is that, a single qualified individual be designated as responsible for overseeing and implementing the information security program. Currently the rule allows multiple employees to be responsible for coordinating the program. The idea behind requiring just one individual instead of multiple employees, was to improve the accountability for information security programs. FTC chair, Lina Khan, and commissioner, Rebecca Kelly Slaughter had issued a joint statement in support of the new rule. And in that statement, they pointed out that Equifax, which had experienced a massive data breach back in 2017, had split responsibility over its information security program between two people.

Doris Yuen:

They considered that to be actually one of the major causes of the data breach because the division authority led to failures in communications and oversight and in enforcement of the program. So the qualified individual required by the new rule can be employed by either the financial institution itself or an affiliate or a service provider. That qualified individual is also required to report at least annually to the financial institutions, board of directors or the equivalent governing body or to the senior officer who's responsible for the information security program.

Doris Yuen:

And the report must include the overall status of the information security program and the compliance with the rule and material matters related to the program, which include issues such as risk assessments, risk management, and control decisions, service provider arrangements, the results of testing security events or violations, and the managements responses to such things. And also recommendations for changes in the information security program. In the notice of proposed rule making that FTC had sought comments on whether the board or equivalent governing bodies should be required to certify the contents of that report, but the rule that was issued does not show certification requirement at this time.

Doris Yuen:

The rationale behind leaving that out from the rule was that requiring the governing board to certify the contents of the report would likely transform the report into a compliance document. And that might reduce its efficacy as a communication between the qualified individual and the board. Now I'll turn it over to Kim who will talk about additional requirements for the information security program.

Kim Phan:

Thanks Doris. So again, the rule makes changes in five specific areas, and I think the most substantive of those changes are going to be found in the updates to the information security program requirements. So, what do they require? Previously, as Doris had already flagged, financial institutions were required to scope the nature in what they did as far as data protection and safeguards around, again, the size of their organization and other types of risks, such as the sensitivity of the customer transaction information that they have.

Kim Phan:

What the new requirements require is that those risk assessments, while previously might have been more flexible in context of, again, a feel for the nature of your organization and the risk posed to it, now those risk assessments have to be much more formalized. They have to be conducted on a periodic basis. The FTC doesn't go so far as to say whether or not they have to be annual or more frequent such as on a quarterly basis or even every other year, yet there is some flexibility built into the new rules, even though they, again, are very prescriptive.

Kim Phan:

But when you do conduct that risk assessment, the assessment itself has to be written. It's not enough to just have a feeling for what risks are out there and to assign safeguards to protect data from those risks. You now have to document very specifically the identification of each risk and the specific step, the safeguard you're putting into place to mitigate that particular risk or whether or not you are accepting that risk. And to a certain extent, accepting some risks is a reality in the current digital world. So, the FTC does accommodate for that within the rule making as well.

Kim Phan:

Some additional requirements in the area, the access controls. Access controls are the safeguards that are designed to authenticate how authorized users can access customer information on your network. Keep in mind that the FTC rule is also not just limited to technical safeguards to network access, but also is relevant to physical safeguards. Not only do you have to think about access controls to information systems, but also physical controls over paper records and physical devices like laptops, thumb drives.

Kim Phan:

And a lot of what you see in the access control language in the new rule arises out of many of the FTCs past consent orders relating to access controls, for example, internal users not being given administrative control unless there's a clear specific reason, not allowing external users to store their passwords in clear text. A lot of this is driven by the FTC's past consent order. So some of this is not a huge surprise, but again, just a more detailed description of what their expectations are.

Kim Phan:

There is a clear expectation that you develop an inventory, data inventory, a documentation of all the data that you as a financial institution possess. And while they don't use the term data map, it's pretty clear from the FTC requirements as laid out in the new rule, is that what they're expecting you to develop, that you map out all the incoming data sources from which you're collecting personal information, how you're storing that internally, how you're using it internally, where you're transmitting it externally, and basically laying out not only the inventory of what data you have, but how it flows from, into, within and out of your particular financial institution.

Kim Phan:

The FTC also anticipates that once you have that map in place, that you are going to make an assessment as to the relevant importance or criticality of each of the system identified in that data inventory. So again, it will be a heavy lift for some smaller entities to be able to do that sort of thing. Now there are of course manual processes that can get you to the same place, but there's also software, they can get you there. Those can be very expensive, but there are options, but some of those may be hard for smaller entities.

Kim Phan:

Encryption. The FTC is memorializing its expectation in these requirements, that encryption be present, not only in transit when data is flowing into or out of your organization, but also at rest within your organization itself. Now the FTC doesn't prescribe a specific technology for encryption or a process, they don't lay out 128 or 256 bit encryption just simply stating that

there has to be encryption, again, a prescripted requirement, but with some flexibility, as far as what that type of encryption has to look like.

Kim Phan:

Secure application development, that is a strict requirement now under the new FTC safeguards rules, but again, reflected in past FTC enforcement actions, to the extent that you have software being developed in house, you would have to have appropriate training for those folks on how to develop applications that will be running on your network that access personal information, but as well as having oversight, a third party developers as well. If you're engaging a service provider to build out a new application on your website or in a mobile app, you want to make sure that you have processes in place under the safeguards rule to securely test any externally developed applications.

Kim Phan:

Also, multifactor authentication. The FTCs expectation here is not only that you have multifactor authentication for external access to customer information, customers themselves logging into your platform, but also MFA for internal access, your own employees, but it's not limited just those, there's also third parties that the FTC contemplates. Some of your business partners or service providers or others, anyone else who might have access to personal information in your system, the baseline expectation is going to be that those individuals access that data under an MFA process.

Kim Phan:

One helpful note that the FTC includes in their rule and their discussion of the rule is they do specifically state that a process that includes requiring a password, entering your username, a password into a website, and then entering a one time code that gets delivered to say a consumer cell phone, or say a key fob that an employee may hold, that specifically, the FTC recognizes as satisfying this requirement. So, to a certain extent, the FTC is trying to be helpful where they can.

Kim Phan:

Some additional information on security program requirements laid out in the new rule, secure disposal. Now the FTC doesn't lay out specifically retention periods, how long you do have to keep something, there are different business operational and legal requirements for different types of data and how long you have to retain it, but the FTC does lay out that once that retention period has expired, there is a clear expectation that you remove, delete or destroy that data in a very secure way, and that whatever your retention period is, it needs to have a legal basis, and that you are being thoughtful about the medium from which that data has to be destroyed, whether or not it's your network, whether or not it's being wiped from a laptop, or even that, say copy machines that you use that you might you've made copies of consumer applications. Those need to be wiped as well.

Kim Phan:

Having appropriate change management processes to ensure that your safeguards again are keeping up to date with any new devices that you're adding or removing from your system, any integration of new software's, or maybe new entities, if you merge or acquire a new entity, anytime you update your software, that you are, again, keeping mindful of how that might impact your broader safeguards that might have interdependencies with any of those software's or technologies hardware's.

Kim Phan:

Monitoring and logging user activity. Now, there should be, one, either continuous monitoring, and the FTC gives you this option, either one continuous monitoring, mealtime, ongoing monitoring, or two, annual penetration testing and vulnerability assessments. So you can do one or the other. Continuous monitoring or penetration testing and vulnerability assessments. But you have to do one or both.

Kim Phan:

Having user activity logs, having those logs in place so that you can recreate consumer transactions should something go wrong with your systems, should you be attacked by ransomware, other types of activity needs to be retained and saved for a certain period of time for the protection of your customers, as well as from validating, if there's been unauthorized access or tampering with that data that you can recover the underlying logs that show what the content of your data should be.

Kim Phan:

Information security personnel. The FTC flags that not only do you have to have a qualified individual overseeing your overall information security program, each of the individuals within that information security program have to be qualified for the position for which they have been assigned, and the job responsibilities for which they are being given. Now, that could be a challenge for many of you who are staff challenged to look for folks with the right types of expertise, but there is a clear expectation from the FTC that you have those folks in place.

Kim Phan:

Training. Now, the FTC expectation is not only that you have baseline training for all employees. Now, again, they want this to be an enterprise ride consideration from the CEO all the way up to the lowliest intern, everyone gets security training. But the FTC also expects that you have enhanced training for those in say, security roles. So you have to think about to what extent you need to have tailored training based on the job and job responsibilities of a particular individual within your organization.

Kim Phan:

Service provider oversight. Again, another very important issue for the FTC and something that they have focused on in past consent orders. What that looks like including initial due diligence, strong contractual protections, ongoing monitoring, auditing, as well as monitoring consumer complaints that may arise with regard to any particular service provider. Having a written incidence response plan, Doris mentioned this earlier, again, to the extent you may have processes and procedures, if your company experiences some sort of data breach or other type of incident, the FTC now says that plan has to be written out.

Kim Phan:

It has to set specific goals for what you're trying to achieve in responding to an incident, what your internal process will look like, who is responsible for what stage of an incident response, who has decision making authority, say, for example, if your website has to be taken down, or if a system or server has to be taken down for maintenance. How you communicate about breaches internally with your employees, as well as externally with customers, regulators, states, and other entities remediating, having a post incident action plan as to how you will address any issues that were identified during the incident, as well as documenting all of it.

Kim Phan:

A lot of what the FTC is requiring is, again, a lot of documentation of process. So, can get very, very complicated, very, very quickly. Now, leaving the definition ... Excuse me, leaving the exact changes to the information security program, we're next going to talk about an expanded definition of financial institution. Now, for those of you who've been wondering about the scope of this particular rule, keep in mind that the federal trade commissions scope and jurisdiction is over essentially all interstate commerce, with the exception of banks and nonprofits.

Kim Phan:

So if you are a bank, the FTC new safeguards rule does not technically apply to you, but keep in mind that when the FTC first issued their safeguards rule way back in 2000, the other prudential regulators on the federal level issued inter agency guidance that basically tracked what the FTC put together. That was the Fed, the FDIC, the OCC, all that together. While there were a

few tweaks that were specific to banks, such as filing of SAR reports, the framework was essentially identical. So, for those of you who are banks, keep in mind that this FTC rule will probably be very similar to what the other regulators will be imposing on you very, very soon.

Kim Phan:

However, for those of you who are not banks, the breadth and scope of financial institutions that are covered by the new FTC safeguard rule includes mortgage lenders, payday lenders, check cashers, collection agencies, CRAs, investment advisors. All of these folks are generally going to be falling under the scope of the FTC. And further the FTC has expanded the definition of financial institution and include activities incidental to financial activities. Now, incidental to financial activities could be a lot of different things. Don't worry. It's not quite as broad as it sounds, specifically, finders are entities that the federal reserve board has in its own rule making, determined or engaged in activity that is incidental to a financial activity. And that's the key.

Kim Phan:

This expansion only covers entities that the federal reserve board has or will eventually rule incidental to financial activities. And finders are the only entities so far that the federal reserve has issued a rule about. So, what's a finder? Right? A finder is defined as an entity that brings together buyers and sellers of products or services for transactions that the buyers and sellers themselves negotiate and consummate, because these entities are collecting, maintaining and storing a lot of sensitive consumer information, and it is related so closely to an actual entity providing a product or a service that is financial in nature to a consumer, the Fed included them within the scope of what they consider incidental to financial activities.

Kim Phan:

So again, it sounds broad, but it's not quite as broad as it might otherwise sound, finder being kind of a generic term. For purposes of GLBA, the product that finders are batching buyers and sellers with, have to be for personal, family or household purposes. And also, finders have to be related only with regard to customers and consumers. So under GLBA, it is pretty narrow, but significant, the FTC expanded its rule to include them.

Kim Phan:

Other definitions. So the FTC at the time that GLBA was enacted and was issuing these rules as Doris described earlier, the privacy rule and the safeguards rule, the FTC had jurisdiction over both. Now, when Dodd–Frank came along in 2010, it actually bifurcated the GLBA, the privacy rule went primarily to the CFPB and the CFPB has primary jurisdiction over that particular rule. The safeguards rule, the FTC was able to argue, "We are the defacto data security regulator. We have long experiences area. The safeguards rule should stay with us."

Kim Phan:

So in Congress's infinite wisdom, they set the privacy rule to the CFPB and the safeguards rule stayed with the FTC. However, because of the time, 10 years prior, the FTC had issued these rules initially, they were interdependent. So a lot of the definitions that were in the safeguards rule simply referred to the definition as laid out in the FTCs privacy rule. Now that the FTC no longer has jurisdiction over the privacy rule, they've decided to insert new definitions into the safeguards rule, which really just piggybacks off the privacy rule, but keeps them in two separate places, so they're not cross referencing each other.

Kim Phan:

They've also added some additional definitions picked up from New York DFS and the NAIC as Doris had flagged earlier, which are the basis for the new safeguards rules updates, things like authorized user, security event, they have a specific definition for encryption, multifactor authentication and penetration testing. Prior definitions under the safeguards rule, things like information security program and service provider remain unchanged. But lot to be seen in the definitions if you're looking to update your compliance. With that, I will toss it back to Doris, then we will cover some last things that we wanted to flag for your attention.

Doris Yuen:

Thanks, Kim. The FTC recognized that the additional requirements that Kim just discussed may play, say, significant burden on smaller financial institutions. So to help reduce this burden, the new rule provides a limited exemption from certain requirements for smaller institutions, the rule exempts financial institutions that maintain information on fewer than 5,000 consumers from certain requirements such as the written risk assess, the requirement to do continuous monitoring or annual penetration testing and biannual vulnerability assessments.

Doris Yuen:

These smaller institutions would also be exempt from the requirement of having a written incident response plan, and to have annual reporting by the qualified individual. Now, this is not a complete exemption, smaller financial institutions would still have to do certain things. For example, they would still need to conduct risk assessments even if the risk assessment wouldn't be required to be memorialized in writing. They'd also have to design and implement a written information security program with the required elements and utilize qualified information security personnel and train employees.

Doris Yuen:

They'd also have to monitor the activity of authorized users and oversee service providers and evaluate and adjust their information security program. The FTC also recognized that certain of these requirements may take a while to implement. So they push the effective date of certain provisions out to one year after the date of the final rule is published in the federal register. These include requirements relating to the appointment of a qualified individual and their annual written reports to the board, also includes the conducting of a written assessment and the requirement to do continuous monitoring, penetration testing and vulnerability assessments.

Doris Yuen:

It also includes the required training for personnel and the periodic assessment of service providers. It also includes the written incident response plan and certain other new elements of the information security program, such as the access controls, the data inventory, the encryption, the secure application development practices. None are the other requirements that can discuss such as the multifactor authentication, disposal requirements change management and monitoring and logging of user activity.

Doris Yuen:

So the remainder of the provisions are effective 30 days following publication in the federal register. The elements that would be in fact immediately after the final rule is published, are what's already required under the current rule, such as the requirement to have a written security program and to conduct a risk assessment, even if that's not required to be memorialized in writing. So financial institutions would also need to design and implement safeguards to control the risks identified in that risk assessment.

Doris Yuen:

They also need to regularly test or otherwise monitor the effectiveness of the safeguards key controls, the systems and the procedures. They would also need to oversee service providers at the onboarding stage and to evaluate and adjust the security program in light of the results of that testing and monitoring. Then I'll turn it back over to Kim to talk about criticisms of the final rule.

Kim Phan:

Thanks Doris. So, we'd be remiss if we didn't note that these changes to the safeguards rule have been quite controversial, to say the least. The final rule has been approved along party lines. All of the Democratic commissioners voted in favor, both of the Republican commissioners dissented. It was the same when the rule had been initially proposed. While there has been an extensive period of comments, the workshop as Doris noted, this process started years ago, and yet despite all of the industry

pushback and others who have questioned the need and the effectiveness of these updates, the rule essentially has been finalized very similar to as it was initially proposed. And that was quite problematic for the Republican commissioners.

Kim Phan:

Essentially, they argued that, having such prescriptive requirements stifles innovation, entrenches incumbents by handicapping smaller players or newer entrants. Right? So yes, there is a 5,000 or less consumer small business exception, but that's in practical terms, that's almost no entities in the financial institution or financial industry. Right? It's not even a realistic option for most entities that as on a regular basis operate as a financial institution.

Kim Phan:

And interestingly, the commissioners, the Republican commissioners noted that this was one of the rare instances where they saw both privacy advocates and the largest financial institutions form an unlikely alliance in that they were both pulling for the FTC to establish very detailed requirements. They knew some of the smaller midsize players might not be able to build out within the timeframe as Doris described within the next year.

Kim Phan:

The Republican commissioners also argued that being overly prescriptive doesn't even make sense in an area like data security, where standards are continuously evolving and that the FTC, which for years and years and years has based its rule makings on data, weighing the costs and the benefits and having the data to support arguments on both sides. The Republican commissioner said, "We just don't know enough about whether or not the safeguards rules as they were previously established, the flexibility that they had, well, had failed in any respect or that whether or not the new rules and changes to the safeguards rules would actually improve data security overall and actually protect consumers data more than where they are today."

Kim Phan:

Furthermore, at the time that this rule making process started, keep in mind, the New York DFS and NAIC, both released the cybersecurity regulation and the model rule in 2017 at the time that the proposed rule making was issued by the FTC, which was back in 2019. In those two years, the Republican commissioners pointed out, like there's just not enough data about how companies have implemented it, whether or not there have been issues operationalizing the requirements and whether or not they can be effectively used to enforce consumer protections against those who are not properly securing data.

Kim Phan:

Furthermore, the Republican commissioners charged that the FTC was essentially substituting its own judgment for what private companies should be able to decide on their own. What should be the level of a board overall engagement, or should it be a board subcommittee? What should be hiring and training requirements for a company? Do you have to hire someone with all of these qualifications or can you train someone in house to have the expertise to be in certain security roles? As well as how to hold individuals accountable within the organization for any lapses in data security?

Kim Phan:

All of that, the Republican commissioners said, companies with their own organizations, with their own relationships with their people are in a better position to figure that stuff out. Finally, the commissioners noted that because Congress is already looking at considering a federal data security law to follow in the footsteps of the states in this area, Colorado, Massachusetts, that it may not be appropriate for the FTC to step in at this time.

Kim Phan:

So, all of these were reasons why the commissioners dissented, they may be the basis for some helpful arguments that companies may be able to raise at a later time if you're having or finding that you're having problems implementing some of, again, these very prescriptive requirements. Also, we should flag that, from industry and those of you, whether or not you

submitted comments on your own or whether or not you worked with some of your trade associations to submit public comments on all of your behalves, all of them reflected many of the same concerns that the Republican commissioners raised, that prescriptive requirements would not result in any kind of material benefit in security or increase consumer protection, or even decrease the likelihood of various types of data breaches. Right?

Kim Phan:

That the reality is, many of you are probably doing some of these steps anyway, this is out of the extra compliance burden and devoting staff and resources to documenting things that otherwise they could be actually protecting data. So, another issue that was raised in the public comments that the Republican commissioners also highlighted was the fact that a checklist approach and one size fits all for companies really just sets a minimum threshold. Right? Some companies are going to do the bare minimum what they need to do and call it a day.

Kim Phan:

Whereas in the prior approach, if you are a larger entity with more resources and more consumer data, you might actually go above and beyond that and impose additional safeguards that go beyond what the FTC is proposing here, but now there'll be no incentive to do that. It also creates a roadmap for bad actors. They know exactly what most financial institutions are going to do, the bare minimum, and they have to just get over that hurdle, if they can overcome that, then they're going to be able to walk into most financial institutions and steal data. So again, not that helpful to consumers.

Kim Phan:

The last thing that they flagged was, the NIST, the National Institute of Standards and Technology, a few years ago, they established the cyber security framework. Right? It is a very robust, voluntary standard that has been made available to the private sector and the federal financial institution's examination council actually adapted that cyber security tool by the NIST organization and developed a cybersecurity assessment tool of its own. And the FTC pointed out why aren't we aligning our safeguards rules with what the FFIC already expects from financial institutions and other in this industry.

Kim Phan:

So again, a lot of criticism to be thrown at these safeguards rules, again, a lot of these criticisms resulted in an actual changes to what the proposed rule making was to the final rule making. But it's good context so that you know what might have been, and also provides you with some ammunition in the event that the FTC ever looks in your direction. Finally, what we're going to cover is just some last helpful tips. What to be thinking about going forward from here. As Doris laid out, there are some of the requirements in the safeguards update that will go into effect immediately once published in the federal register.

Kim Phan:

But most of the new changes and the prescriptive requirements, you'll have a year to put into place. So what are some of the things that will probably be the heaviest list and things that you should start moving on right away? As we talked about data mapping to the extent that you haven't already done that, can be an immense time requirement of both personnel and resource to try to map out all of the data flows and data inventories for customer information that you may be holding, that can be a lengthy process. So it might be prudent for you to start thinking about how to set up that now.

Kim Phan:

Thinking about how to modify any internal processes and accountability procedures, as far as the reporting, what that format looks like, what you're monitoring and auditing looks like, whether or not you're going to do some of those things in house or whether or not you are going to outsource some of those functions to third parties, such as the written risk assessment, the ongoing monitoring and auditing, the vulnerability assessments, the penetration testing, all of these are very prescriptive steps that you would think about whether or not you could do them in house, but even if you decide to do them in house, one thing to think about is you might want to consider bringing in a third party periodically. Right?

Kim Phan:

Maybe not every year, but maybe you want a third party to validate the types of penetration tests you've been doing, or to validate the types of audits you've been conducting. To the extent that you bring in any of these third party service providers, again, keep in mind, there are a lot of new requirements that the FTC expects of financial institutions in overseeing those service providers. So whether or not you have a long term contract, or just a year contract with a particular service provider, you need to be thinking about for purposes of amendment or renegotiation, how to incorporate some of these new security expectations into your relationships and documenting them with your service providers.

Kim Phan:

Now, the reason a lot of this is going to be very, very important is that we expect to see the FTC continue to focus on privacy and data security issues on a going forward basis. Their primary authority here is to bring enforcement actions. Right? So, as soon as this safeguards rule goes into effect, I think we can expect the FTC to move very quickly to try to find opportunities to make headlines with regard to being the toughest cop on the beat. Again, keep in mind the FTC has a complex from the reality that a lot of its jurisdiction was given to the CFPB.

Kim Phan:

The CFPB very traditionally has been very quiet with regard to privacy and data security issues, but now that it is increasingly a focus of not only consumers, but also the state, we can't expect maybe the CFPB to start focus on this more. And while the FTC and the CFPB are intended to coordinate, I think you will see some gamesmanship here, one trying to show up the other one with regard to how strong they can come down on enforcement. And we have some questions here about where the FTCs new safeguards rule stacks up against some other standards.

Kim Phan:

I would say New York DFS probably continues to be probably the most stringent as far as what it lays out and what its expectations are. The FTC, again, modeled much of what it has done here in the safeguard rule on what the New York DFS did, but not quite as strict. Then the CFPB pulling up the rear very quietly, but with no fanfare, no press release, no blog, nothing like that, released an update to its supervision and examination manual last month. Well, excuse me, not last month, in September, with regard to IT examination procedures that its examiners would be asking questions off when doing supervisory exams of financial institutions.

Kim Phan:

So, for example, New York DFS requires logs to be maintained, audit trails of financial transactions, depending on the nature of the transaction and the information being logged, New York DFS dictates that certain types of those logs be retained for three, five or six years. Now, again, the FTC one step below also requires logs. Doesn't specify how long those logs have to be retained, but does make the logging requirement something that is marginalized in the safeguards rule. Then the CFPB pulling up the rear again, simply ask the question, "Are you maintaining logs? If you're not maintaining logs, what are you doing besides that or elsewhere?" Right?

Kim Phan:

So, that's how I would stack them up against each other for now. I think there's still to be seen whether or not New York DFS in enforcing its own cybersecurity regulation has only brought what? Just a handful, less than five enforcement actions under that particular rule in the last four years, how quickly the FTC moves to enforce its rule and whether or not the CFPB, we see things in their supervisory highlights or other exam reports that show that they are focusing a lot on this area, all of that, yet to be determined, this is certainly an area flux where there's going to be a lot of changes to come.

Kim Phan:

Another important thing to note about the FTC is, there's a lot of congressional interest in enhancing the FTCs authority in the privacy and data security space. You've probably seen that they build back better. President Biden infrastructure bill includes funding for the FTC to create an entirely new bureau of privacy, which would also include data security. This would be in addition to its existing Bureau of Competition and the Bureau of Consumer Protection. If that happens, the FTC will have more staff, more resources, more money to pursue enforcement actions under this particular safeguards rule.

Kim Phan:

Also, the FTC has called four years and starting to get some traction in Congress for them, the FTC to be giving more stringent and more expansive rule making authority. Now, again, the FTC has broad enforcement authority, but very limited rule making authority only under certain statutes, are they given the authority to issue rules like The CAN-SPAM Act, and here under the GLBA where they issued the safeguards rule, but they would love to have the authority to issue broader UDAP, unfair and deceptive acts and practices authority type requirements for all interstate commerce, with regard to privacy and data security.

Kim Phan:

So, if we see the FTC receive that type of authority, I think we can expect the FTC to take immediate actions on that as well. So, all of you should be thinking very carefully about all of those steps and thinking about how you are going to be building out your information security programs over the next year in order to satisfy the safeguards rule. The one thing that we wanted to cover before we let you guys go today, is that at the same time that the FTC released this update to the safeguards rule, they issued another notice proposed rule making with regard to the reporting of data breaches.

Kim Phan:

So, the supplemental rule making would essentially lay out under the safeguards rule when a financial institution would have to notify the FTC of a data breach or security event. Right? A security event being defined as the misuse of customer information that has, or is reasonably likely to have a negative effect on consumers. Right now there's no reporting requirement at all. Now, some of the other financial regulators, the FDIC, the OCC, treasury have issued interagency guidance on when they, as the supervisory entity of banks, need to be notified if there is a security incident, but the FTCs never issued or required a similar notification to be provided to them for the financial institutions, for which they have jurisdiction.

Kim Phan:

So they're floating out this new proposed rule making that they be notified. It would only be triggered if a particular risk event impact a thousand or more concerns nationwide, that notification to be provided to the FTC as proposed to the rule making would be via an electronic form posted to the FTC website. And like some of the states, not all of them, some of the states say California, every notice and all the information being provided in that notice would then be come publicly available. The FTC would release these in a publicly available database, very different from how they set up their Sentinel database, which is the repository of consumer complaint data.

Kim Phan:

These notifications of data breaches would go on this publicly available database and be seen by everyone. Now, that notice proposed rule making is an invitation for public comment. The public will have 60 days to submit comments in response to that rule once it's published in the federal register, again, nothing published yet, may take a little while, it's over the holiday season. Of course, it's COVID. But for those of you who are chafing over the idea of the many other steps already laid out the safeguards rule for you to handle, if you have any hesitation at all about adding another regulator to the list, already extensive list of state regulators, that you have to notify in the event of a breach.

Kim Phan:

Think about whether or not it makes sense for you to submit public comments in response to this expansion of the safeguards rule. That is what we have to cover today. If any of you would like any assistance or support with regard to building out your safeguards program, to comply with the rule, please feel free to reach out to myself, Doris, or reach out to Alan. And finally, for those of you who are interested in tracking privacy and data security developments, Ballard Spahr has a tracking service specific to the consumer financial services privacy and data security developments.

Kim Phan:

That tracker service includes weekly updates with everything that's happened in the world of consumer privacy and data security for financial institutions, as well as monthly round table calls, where we discuss with our subscribers, what has been happening, what they should be paying attention to, and really deep diving on some of those developments, as far as what operationally some of those impacts may be. If you're interested in running or subscribing to that tracker, feel free to reach out to me, I'm happy to get you additional details about that.

Alan Kaplinsky:

Well, we've come to the end of our podcast show today, and I want to thank Kim and Doris for just doing a terrific job on explaining these new updated GLBA safeguards rule. And just remind our listeners that we have a new podcast show every week, except during Thanksgiving week and except during Christmas week. So we do 50 shows a year. You can find our podcast show on basically any platform where you access podcasts. You can also find it on our website, but it's available on Google Play, Spotify, et cetera.

Alan Kaplinsky:

We have been doing this podcast show now for over three years, and we recently won an award by a company that rates podcasts programs of law firms, and we came in, I'm very proud to say, second in the country. Finally, in addition to thanking Doris and Kim, I, especially, want to thank all of you who took the time to download our podcast and listen to it today. I hope you also consult our companion blog, which also goes by the name of Consumer Finance Monitor. We cover a lot of the same topic on the blog that we cover on our podcasts and our webcasts. Thank you again.