Consumer Finance Monitor (Season 2, Episode 17): A Look at the FTC's Proposed GLBA Rules

Speakers: Alan Kaplinsky and Kim Phan

Alan Kaplinsky:

Welcome to Ballard Spahr's, Consumer Finance Monitor podcast. I'm your host today, Alan Kaplinsky, the chair of our consumer financial services group at Ballard Spahr. And today I'm very pleased to be joined by my partner, Kim Phan, who is noted for her work in the area of privacy and data security issues for a variety of industries, most notably consumer financial services. Kim previously practiced at our firm for more than four years, left for a short period of time and then recently rejoined us as an integral partner in our privacy and data security group, which helps our clients across the country, navigate the many laws designed to safeguard health, financial and other private information. And as I indicated earlier, she will work and has worked very closely with our consumer financial services group, employing her significant experience in consumer finance law and her familiarity with eCommerce, mobile payments, data analytics and other areas of FinTech. Well, welcome to our program, Kim. Welcome.

Kim Phan:

Thanks Alan. It's my pleasure to be here.

Alan Kaplinsky:

We're going to have a discussion today about a recent proposal of the Federal Trade Commission amending two of Gramm–Leach–Bliley Acts implementing regulations. Can you describe for our audience, which ones we're going to be talking about?

Kim Phan:

Certainly, Alan. The two proposals are with regard to the privacy rule and the safeguards rule. The privacy rule went into effect in 2000 and generally requires financial institutions to inform their customers about their information sharing practices and give those customers the ability to opt out a certain sharing with third parties. The safeguards rule, when into effect in 2003 and requires financial institutions to have a comprehensive information security program.

Alan Kaplinsky:

Kim, does the FTC's proposal for the privacy rule impact the CFPB'S Regulation P?

Kim Phan:

It does not, Alan. When the GLBA was first enacted back in 1999, it spread its authority across the various financial credential regulators, as well as the FTC. When the Dodd-Frank Act was enacted in 2010, much of the FTC's and the CFPB and the prudential regulator's authority was actually transferred to the newly created CFPB. The FTC retained a very narrow section of rulemaking in the privacy space with regard to motor vehicle dealers. Though specifically that don't make extend any kind of credit, which would still be covered by the CFPB. And those are actually the only entities, those motor vehicle dealers that do not directly extend credit, who are impacted by the FTC's privacy rule. Thus, CFPBs Regulation P is not impacted by what the FTC is doing.

Alan Kaplinsky:

Okay. And so let's talk about the privacy rule right now. What changes exactly are they proposing to make?

Kim Phan:

The FTC is actually amending its own privacy rule to reflect the CFPB's Regulation P and to reflect some of the FTC's reduced scope with regard to the privacy rule. Again, removing all references to financial institutions that are not motor vehicle dealers, making some conforming changes to the regulation that the CFPB has issued and otherwise just making some minor technical changes as well as reflecting the regulation to make changes according to the FAST Act. The FAST Act was passed by the Congress a couple of years ago and it allows financial institutions under certain conditions not to have to provide the annual GLBA privacy notices, the one pager that everyone gets in the mail.

Alan Kaplinsky:

That annoying document, that we get every year and never read.

Kim Phan:

Correct. No one reads them. Everyone puts them immediately into the circular file. And this is to alleviate some of the over notification that people are getting of those and to alleviate some of the burden on companies for sending those. If a company doesn't make any changes to their privacy notice, if they are not providing any information to third parties in a form that consumers would otherwise be allowed to opt out in and in some other additional conditions, they no longer have to send the privacy notice. And under the revised rules, neither will motor vehicle dealers under the FTC's new proposal.

Alan Kaplinsky:

Okay. Let's turn now to the safeguards rule. What financial institutions are impacted by the safeguard rule?

Kim Phan:

Well, Alan, as we already discussed, the Dodd-Frank Act transferred most of the rulemaking authority for the privacy rule to the CFPB. However, the Dodd-Frank Act bifurcated GLBA and left the responsibility of rule making for the safeguards rule intact and with the FTC. Thus, the safeguard rule applies very broadly to all financial institutions within the FTC's jurisdiction, which generally means financial institutions engaged in interstate commerce, that are not banks or nonprofits. And thus, that includes payday lenders, debt collectors, check cashers, mortgage brokers and a variety of other non-bank financial institutions.

Alan Kaplinsky:

Let me ask you to clarify something in my mind, Kim, and that is depository institutions, banks. They're not subject to FTC jurisdiction therefore not subject it to the proposed changes to the privacy rule or the safeguards rule. But are you saying that doesn't mean they have to still worry about what the FTC is doing but they do have to worry about rules issued by the CFPB.

Kim Phan:

The banks do have to worry about rules issued by the CFPB. They also have to deal with any comparable safeguards rules that have been issued by their prudential regulators, the FDIC, the OCC and others. And generally those entities, those agencies have combined and formed the Federal Financials Examinations council, which issues an IT handbook and otherwise sets forth data security requirements in a very strict pattern that non-bank financial institutions don't have to comply with and thus, the FTC has the safeguards rule.

Alan Kaplinsky:

Kim, the prudential regulators have their own safeguard rule and the FTC now is proposing to make changes to its safeguard rule. Are they going to be comparable in nature? Or are they going in different directions?

Kim Phan:

It's interesting point you raise, Alan. The FTC did state in its rulemaking that it had consulted with the CFPB and the other prudential regulators in developing its rulemaking. Again, the FFIEC's guidance is very detailed. That is not the direction the

FTC has gone in the past. This rulemaking will move the FTC closer in that direction with more detailed safeguards requirements, as opposed to the more general guidance it's had up until this point.

Alan Kaplinsky:

Exactly what changes are being proposed to the safeguards rule by the FTC?

Kim Phan:

The safeguards rule had required that financial institutions have a comprehensive information security program that was written, that contained administrative, technical and physical safeguards that were appropriate to the size and complexity of the financial institution, the nature of its activities and the sensitivity of the customer information that it was maintaining. The new rule dictates that that information security program had very specific elements to it, where otherwise the financial institutions were able to make their own decisions about what controls they put into place. Now they have to have a written incidents response plan. They have to appoint a CISO, a chief information security officer who report annually to the board. They have to have access controls for authorized users. They have to encrypt personal information in transit and at rest. They have to adopt secure development practices for internal applications. They have to impose multifactor authentication for any individuals accessing personal information. That includes employees as well as customers accessing their own information. They have to have audit trails. They have to have secure disposal procedures. They need new vendor oversight procedures and a variety of other requirements, Alan. It's extensive in that regard.

Alan Kaplinsky:

Okay. Now there is a small business exemption. Am I right?

Kim Phan:

Yes, Alan. Small businesses that maintain personal information on their customers of less than 5,000 in number are exempt in some respects from the requirements to the safeguards rule. It is not a complete exemption. They still have to do some things under the rule.

Alan Kaplinsky:

Okay. You're saying regardless of how small a business is, it could be a small mom and pop grocery store, could be anything, a clothing store, they all have to comply with some parts of this rule.

Kim Phan:

That's right, Alan. They still have to conduct risk assessments. They still have to have a written information security program. They need to give their employees some sort of security training. They need to monitor their users. They have to ensure that there are some appropriate safeguards amongst their service providers, that type of thing. But the FTC actually is seeking comments on the small business exemption. They want to know whether or not the threshold that they've set, 5,000 consumers or less, is appropriate. Whether or not they should set that higher, whether or not they should set that lower. And even whether or not number of consumers is the right standard by which to assess whether or not a company is small. They're asking whether or not they should look at revenue or some other factors in making that determination.

Alan Kaplinsky:

In addition to the small business exemption, whatever it turns out to be, Kim, are there any other exemptions or exceptions provided for in the proposed rule?

Kim Phan:

Unfortunately, at this point, no. The FTC has accepted comments on whether or not there are other standards that might be appropriate. They still haven't determined whether or not any of those will be included in the final rule. For example, a number of commenters suggested that compliance with the NIST cybersecurity framework and or the PCI DSS standards might be appropriate to confer a safe harbor on companies from implementing the more stringent requirements set out in the safeguards rule and the FTC is currently seeking additional comments on those topics.

Alan Kaplinsky:

For our listeners who don't know what those initials mean, can you educate them a bit?

Kim Phan:

Absolutely, Alan. The NIST cybersecurity framework is a framework voluntary in nature that was established by the National Institute of Standards and Technology. It's a federal agency that sets forth a number of different technological standards. They established this a few years ago and a number of financial institutions have already started putting this into place. PCI DSS is a data security standard that has been established by what's called the PCI Council, Payment Card Industry. Essentially any companies, not just financial institutions that utilize payment cards, like credit cards, debit card, and other cards have self regulatory industry standards they're already subject to in this space.

Alan Kaplinsky:

I see. Now the proposed rule, when is the comment period expired? Do you know?

Kim Phan:

Yes. The comment period runs through June 3rd of 2019. And back in August of 2016, when the FTC first initiated this rulemaking, they only received 28 public comments on the safeguard rule. For the broad impact that this will have on the financial services industry, that's a little surprising but there's still opportunity for financial institutions to weigh in.

Alan Kaplinsky:

Right. And I would think that they would. That is a shockingly low number that I would think this time, people are going to be much more tuned into it than they were in the past. Don't you think?

Kim Phan:

I would expect so. And the FTC actually is a little divided already on the safeguards rule. Two of the commissioners, the Republican commissioners have actually dissented from the issuing of this rule. And so any materials that financial institutions can submit in their public comments that could further bolster the position of the dissenting commissioners would be extremely helpful in impacting the final rules when they come out.

Alan Kaplinsky:

Kim, what happens to a company that doesn't comply with either the privacy rule or the safeguards rule issued by the FTC? Do they have to worry about the FTC going after them in an enforcement matter?

Kim Phan:

They do, Alan. When the CFPB again, took some aspects of rulemaking authority under GLBA, but the FTC and the prudential regulators all retained full enforcement authority to bring civil penalties and other enforcement actions under GLBA.

Alan Kaplinsky:

Okay. And I take it they've done it in the past.

Kim Phan:

They have. Security and privacy have become a touchstone for the FTC. They are the self proclaimed privacy and data security federal regulator in the United States and they take that role very seriously and have brought over 50 enforcement actions over the last 40 years in this space.

Alan Kaplinsky:

Kim, as we wrap it up, I just want to find out from you, is there anything I've overlooked that you'd want to add to the mix today? Or have we covered everything?

Kim Phan:

We've pretty much covered everything, Alan. Again, I would emphasize that the FTC is of two minds right now on the GLBA safeguards rule. Again, the dissenting commissioners have been very critical of the replacement of a flexible approach that allows innovation and flexibility in how companies approach data security with a prescriptive approach that mandates very specific, basically a roadmap to a company's data security protection measures. And any ammunition that they could have to help push back on this safeguards rule as it's currently drafted would be extremely helpful to them.

Alan Kaplinsky:

I take it that one Republican did combine with the two Democrats. Am I right?

Kim Phan:

That would be correct. The two commissioners that dissented were Commissioners Phillips and Commissioner Wilson, but yes, the vote was three to two. One of the Republican commissioners did side with the Democrats on issuing this rule.

Alan Kaplinsky:

Okay. Well Kim, thank you very much for enlightening our audience today and I'm sure we're going to have many other opportunities for you to be on our program because there seems to be no lack of developments in the privacy and data security area. I'm delighted you were on our program today. I'm delighted that you're back at our firm and I want to invite all of our listeners to check out other episodes of our podcast show. We've been doing this now since mid-September of last year. Earlier episodes are at www.ballardspahr.com, as well as listeners ought to make sure they follow our blog, consumerfinancemonitor.com and the blog published by the privacy and data security group. And look for a new podcast each Thursday, except on certain holidays. And as I said, you can get them on our website. You can also get them on your favorite podcast site, be it Spotify or Google or anything else. Thank you, once again.