# Consumer Finance Monitor (Season 5, Episode 36): A Look at Recent Federal Trade Commission and Consumer Financial Protection Bureau Initiatives Concerning Privacy and Data Security

Speakers: Alan Kaplinsky, Greg Szewczyk, and Tim Dickens

Alan Kaplinsky:

Welcome to Consumer Finance Monitor podcast, where we explore important new developments in the world of consumer finance and we talk about the significance of those developments to industry and to consumers. I'm Alan Kaplinsky. I'm senior counsel at Ballard Spahr, formally, for 25 years, a group leader and chair of the Consumer Financial Services Group at Ballard Spahr. And it's my pleasure to welcome everyone to our podcast show for today.

We have a very interesting show today that's going to focus on an extremely important issue, namely data security. And a lot of what we're going to talk about is if all this came to fruition, it would be absolutely mind-boggling and very, very difficult for industry to comply with some of these proposals and some of the guidance that has recently been issued by the Federal Trade Commission and the CFPB.

We're going to start this morning with a discussion of what the FTC has done. And what they have done, and we're going to get into a lot more detail about this, is that on August 11th they issued an advanced notice of proposed rulemaking seeking public input on a host of questions, well over 90 questions relating to what it describes as commercial surveillance or the business of collecting, analyzing, and profiting from information about people in order to determine whether a new rule to protect people's privacy and information is appropriate.

And we're going to spend a little more than the first half of our show today talking about what the FTC has done. And then we will segue into a discussion of what the CFPB has done. It's always been the conventional wisdom of those of us that practice in the consumer finance area that the CFPB had really very limited jurisdiction when it comes to the topics of privacy and data security, at least that's how things have been for about 10 years of the 11 year life of the CFPB. But lo and behold, the current director of the CFPB, Rohit Chopra, who is known for pushing the envelope as far as he can push it to get into areas that he thinks need attention, he thinks otherwise.

And on August 11th, the CFPB published a circular confirming that covered persons and service providers under the Consumer Financial Protection Act can violate the prohibition against unfair acts or practices if they fail to adequately safeguard consumer information. They gave very little additional guidance other than to basically fire this shot across the bow of the ship. They didn't go into any detail about what all that means. And it definitely means more than just complying with the FTC's red flags rule.

Well, let me now introduce to you two of our speakers today, colleagues of mine at Ballard Spahr who are on top of what the FTC is doing and on top of what the CFPB is doing in this area. First of all, let me introduce Greg Szewczyk. Greg is a partner in Ballard Spahr's Denver and Boulder offices, and he is the co-leader of our Privacy and Data Security Group. Greg leverages over a decade of experience in high-stakes litigation to help companies assess risk and comply with the ever-expanding patchwork of state, federal, and international privacy and data security statutes and regulations. Greg helps companies of all sizes, from Fortune 500 companies to startups, to build and maintain their privacy and data security systems.

Tim Dickens is an associate in the firm's Litigation Department located in our Philadelphia office, who focuses also on privacy and data security. He counsels organizations on matters relating to the development of state laws dealing with privacy and data security, such as those recently enacted in California, Colorado, Connecticut, Virginia and Utah, in addition to all the federal rules and regulations that we'll be talking about today. So very warm welcome to you, Greg, and to you, Tim.

Greg Szewczyk:

Thanks, Alan.

Tim Dickens:

Great to be here.

Greg Szewczyk:

It's great to be here. We really appreciate the chance to come in and talk to you. It's always fantastic to not just talk privacy, but talk about how it affects the financial services world in particular.

Alan Kaplinsky:

Yes. Well, again, thanks. And I'm going to start off with you, Greg. So could you provide us with a quick overview of what the FTC's announcement and advanced notice of proposed rulemaking in the data privacy, data security, and the commercial surveillance space deals with?

Greg Szewczyk:

Sure. And Alan, I'll just start by saying that the FTC's announcement, although extremely important, wasn't a huge surprise for those of us in the privacy world. For the past few months, FTC Chair Lina Khan has been suggesting that the FTC was going to increasingly focus on what it refers to as commercial surveillance. I remember a big privacy conference, I think it was back in April, where Chair Khan gave a keynote address and this was clearly an important issue to her and the FTC. But nonetheless, it is an extremely big deal and very important.

Alan Kaplinsky:

The use of the word surveillance, doesn't that speak volumes, Greg?

Greg Szewczyk:

It really does. I mean, both in privacy statutes and regulations to date, surveillance is not the term used for this. We tend to talk about analytical tools. We talk about third-party cookies or tracking devices. But using the term commercial surveillance, I mean, it's a very loaded term.

Alan Kaplinsky:

Yeah, spying. It means spying, right?

Greg Szewczyk:

It means spying. I mean, it has a strong connotation for pretty much anybody. And on top of the strong connotation, the breadth of it is, as we've seen in the announcement, it's just staggering how broad this encompasses. But kind of break it down to, and I know we'll get into it more later, but at a high level, I mean, commercial surveillance refers to how businesses collect, aggregate, protect, use, analyze, and retain consumer data, as well as how they transfer, share, sell it or otherwise monetize it.

And these are practices that virtually every single business that has a website engages in. There are tools that you can use to go see what analytics are on a website. And I can't think of a single time when I've used one and seen zero pop up on that. So by the definition that's there, I mean, the FTC is essentially stating that every single business that has a website is engaging in some form of commercial surveillance.

But just to kind of close the loop on the high level, these rules were announced for the notice of proposed rulemaking back on August 11th, seeking an input on a huge range of questions relating to, we'll use their term of commercial surveillance. And then just on, I believe it was August 22nd the FTC opened up the advanced notice of proposed rulemaking for public comment, which will run through October 21st.

So it was a formal notice, advanced notice of proposed rulemaking seeking comment on a list of various different topics and questions that it said were relevant to this issue of commercial surveillance.

Alan Kaplinsky:

What is the focus of the rulemaking? I said in my opening remarks that it's more than 90 questions and it seemed to cover everything dealing with data security.

Tim Dickens:

So at this point, the FTC's goal appears to be identifying any and all potential harms that could result from online tracking generally. As you've said, as Greg said, this is 95 questions that really cover the entire gamut of online privacy and security concerns. These include a lot of the hot button topics like biometric information privacy, use of artificial intelligence in automated decision-making, potential biases in algorithms, and the collection of use of particularly sensitive information, like medical or financial information. And then also a pretty broad list of questions addressing the potential new protections and harms that might face children and teens online.

Given the breadth of the inquiry, it's unclear at this point whether the FTC envisions comprehensive rulemaking that would address each of these topics or whether the FTC will take a more targeted approach and address issues that present particularly acute harms that they identify in this process.

So going beyond the general nature of these questions, one point that is of particular interest to the FTC is the fundamental issue that consumers do not understand what information is being collected or how it is used. This has been a large focus of Chair Khan who stated in the press conference that Greg mentioned earlier that the notice and consent framework traditionally used by U.S. businesses is likely not sufficient to protect consumer and employee rights.

So we're really expecting a significant discussion of how consumers are notified of online tracking and data use and how this notice ties into the concept of consumer consent for both primary uses of data and secondary uses, like statistical analysis or data aggregation.

Alan Kaplinsky:

So Tim, I take it if this were to get finalized, it covers more than just consumer finance and it covers more than just consumers. Does it cover employees, for example?

Tim Dickens:

Employees are definitely a large focus of the questions in this rulemaking, and we're expecting this to go well beyond sheer consumers. Tracking of employees has definitely been a focus, and the internal tools used to track, analyze, and make some decisions as to employee efficiency and hiring, firing decisions is really going to be a focus of this as well.

Alan Kaplinsky:

Yeah. And I take it, it would also cover businesses, business-to-business transactions. So, I mean, it's enormously broad.

Tim Dickens:

Enormously broad. And I think the breadth of this kind of disguises exactly what the focuses will be. But the breadth would include everything you've mentioned so far.

Alan Kaplinsky:

Yeah. And I guess the other thing we ought to make sure that our listeners understand is it only got through by a three to two vote, very partisan, not bipartisan, very partisan with the three Democrats on the commission voting in favor of releasing it and the two Republicans definitely voting against it. Am I right? This is not an FTC bipartisan effort the way some of the things that they do are.

Tim Dickens:

Absolutely correct.

Alan Kaplinsky:

So Greg, what should companies be doing in response to this gargantuan announcement?

Greg Szewczyk:

Yeah, Alan, the first thing I'd say is keep in mind that the sky isn't necessarily falling right now. This is an extremely long, super broad, likely crossing administrations, years long effort. Under the process that they'll have to go under, under the Magnuson-Moss, from what I've been hearing, the average is around six years to get this done if it would go all the way through.

So a lot is going to change during that time. We could have a different makeup of the FTC. We could have a couple different makeups of the FTC depending on how it is. So although this initial advanced notice is extremely broad, seeing how this process plays out over a number of years, it could significantly narrow. And if it went as broad as it could, we'd also likely see constitutional challenges under the Supreme Court's recent holding in the West Virginia case as to whether or not the FTC has the authority to even issue something that broad.

So even if we were going to assume that it was going to move forward at the scope that it is, there would be big questions. But there are also a couple issues out there that could take the wind out of the sail of the FTC on this issue, both at the federal and the state level.

At the federal level, we've been watching the ADPPA, the American Data Protection and Privacy Act advance through. I mean, I always hesitate to make any predictions on whether any particular federal law especially is going to pass. We're in a midterm election year. Excuse me. There are some key hurdles to the ADPPA, especially with respect to what certain senators have said they would need to see in it to have it advance forward.

But in any event, it's about as far as we've ever seen a comprehensive privacy bill get in Congress. And it does appear to have some pretty broad bipartisan support. So if that passes and the FTC would enforce that, it could kind of render this rulemaking a little bit moot or at the very least put it on the back burner as the FTC would have to be shifting a lot of focuses towards ADPPA enforcement.

Even if the ADPPA doesn't pass, we've got five state laws going into effect in 2023, most of which provide some form of an opt-out for targeted advertising or other types of analytical information that would really be part of the subject of this. And we see more states every year introducing bills in this area.

So in the several years that it would take to work its way through the rulemaking process, we could see more and more states adding on and just make this sort of a FTC-level initiative not quite have the urgency or political benefit that it might have for the FTC as more and more Americans already enjoy some form of choice over these types of issues.

Alan Kaplinsky:

Do you think, Greg, that Lina Khan pushed this through when she did in order to put pressure on Congress to enact the legislation that they're considering right now?

Greg Szewczyk:

I actually don't necessarily think that was the case. And from what we've heard, and you mentioned that it was a three to two vote, the two dissenting commissioners actually kind of said the opposite, which is putting this forward is going to kill the ADPPA because it is a... Anytime you have a bipartisan bill, and I'm no political expert, so I don't want to represent myself as that, but anytime you have a bipartisan bill, you're walking a nice edge in a lot of ways and you're making a lot of deals to try to hold different parties together.

And some things that have been said by both the commissioners and by some Congresspeople is, "Well, why do we put our necks out on a bipartisan bill like this and work so hard if you're just going to go and issue some rules on your own?" "What incentive do we have to reach a bipartisan resolution if we have to have the worry that the FTC will just do what we didn't agree to by virtue of its own rulemaking authority."

So I'm not sure that this actually does put pressure to pass the ADPPA. But time will tell.

Alan Kaplinsky:

The other thing, you mentioned a bunch of state laws. And I mentioned in my introduction that both you and Tim and your privacy group has been tracking all the different state laws that have been enacted in the last year or so. As I understand it, and correct me if I'm wrong, those state laws have exemptions for financial institutions. Am I right? Like banks don't have to really worry about the state laws.

Greg Szewczyk:

Well, you're correct that there are partial exemptions under the California law and there are full exemptions under the other laws. When we talk about the state laws, right now the two that we really focus on are California and Colorado. And the reason for that is those are the two states where in California the new agency that was created and in Colorado the attorney general office are issuing regulations. The other three states, Connecticut, Virginia, and Utah won't have regulations implementing their laws.

So under what we'll call the Colorado model, there is a clean exemption for financial institutions regulated by the GLBA. Under the California model, it is only non-public personal information that is exempted. So you kind of have this dual structure. And that's how it has been under the CCPA, what is existing. That will be replaced by the CPRA starting in 2023, which goes above and beyond.

But you ask this and it's actually extremely timely because while there has been this dual situation and while analytics tended to fall under the CPRA rather than the GLBA, just this past week was the end of the California legislative session. And there had been a couple bills that would extend an employee and B2B exemption that had been in the CCPA. Those bills did not pass. So what you have been talking about with the employees, that is all going to be covered by the California privacy law and will not be exempted because it won't constitute NPI under the GLBA.

So all of this analytics surveillance, any other terminology that you want to use, with respect to California employees of financial institutions, that's all going to be covered under state law starting in 2023.

Alan Kaplinsky:

Yeah. Let me just add one additional thing to all the various obstacles that you mentioned that this rulemaking is likely to face. So many years ago, when Congress was not very happy with the FTC because the FTC was being very heavy-handed in the way it was regulating and in the way it was interpreting Section 5 of the Federal Trade Commission Act dealing with unfair and deceptive acts and practices, they enacted something called the Magnuson-Moss Act, and they basically, it was Congress's way of punishing the FTC. And what they did, they said from now on when you issue regulations FTC, unlike at every other agency, you have to follow not only the Administrative Procedures Act, but you've got to follow our new rule that we, Congress, are subjecting you to.

And basically, what it is, is that instead of proposing a rule and giving interest groups in the public a chance to weigh in, the standard procedure under Magnuson-Moss requires the FTC to give Congress a heads up before rulemaking. It's got to hold a hearing with experts who speak to each side of an issue, and it's got to keep more detailed records of meetings with outside groups.

And while rulemaking at the FTC had been a very slow process when they didn't have to comply with Magnuson-Moss, and in some areas they don't have to comply. They're doing a proposed rulemaking right now that would pertain to automobile dealerships and they don't have to comply with Magnuson-Moss. It generally takes three years for the FTC to issue a final rule. When they have to comply with Magnuson-Moss, it's six years.

So as you point out, if the administration should change, we're controlled by the Republicans in 2024, the composition of the FTC will change, and all this could very well go away.

But let's turn now to an agency that's already done something. This isn't an advanced notice of proposed rulemaking. It's not a proposed rulemaking. It is an announcement by Rohit Chopra, the Director of the CFPB, something that he did by fiat, only he was the only person who he had to consult with. There's no commission. It's one leader at the CFPB. And he issued

something called a circular. And I'm going to start first with you, Greg. Can you give us a high-level overview of what the CFPB circular announcement contains?

Greg Szewczyk:

So the CFPB circular at the highest level stated that covered entities may violate the CFPB's prohibition on unfair acts or practices when they fail to adequately safeguard consumer information. I think there are a couple, there are in my mind at least two high-level points worth focusing on at that even before we start digging in.

And the first is that unlike other data security regulations, like the FTC's updated safeguards say, where the trend has been moving towards requiring specific security standards, the CFPB's instead pushed back and gone more in the reasonableness standard even though it did cite some examples of what could be required. And I think that's a very significant thing that we'll talk about a little more in a minute.

The second is that the CFPB makes clear that actual injury to consumers is not necessary for a company to violate this standard. Instead, it's the risk of potential harm that's sufficient. We usually see that standard discussed in data breach litigation, as to whether or not any harm has been suffered. But in the context of this circular, it can be read to mean that the CFPB could bring an action against a company for inadequate security measures even though there has not been a data breach or any other incident, just strictly for the failure to comply with its reasonableness standard for data security incidents. So I think that's a very big point that comes out of this circular fiat.

Alan Kaplinsky:

Yeah. Well, I guess I could say from someone like myself who has been spending the last 11 years of my career with a very heavy focus on the CFPB, I guess I could say I'm not surprised at all by what you've said.

So Greg, I earlier said that the CFPB didn't give any guidance at all of what it considers to be adequate security measures. Is that 100% accurate? They basically said if your security measures are unfair the way the word unfairness is described in the Consumer Financial Protection Act and we will decide using that definition of unfairness whether or not you have violated the law. Is that really all they've done? That's pretty pitiful.

Tim Dickens:

I can actually jump in here and address this one. So they do provide some information as to what would likely not be considered an adequate security measure. The final section of the circular highlights three fundamental measures that are really critical to any security program. And these measures are multifactor authentication, appropriate password management policies and procedures, and timely software updates.

So an important part of this, the CFPB highlighted that multifactor authentication should not only be required for employees handling customer information, but should also be provided as an option to help secure consumer accounts or customer accounts. So this focus is not only on the back-end security of the business's systems, but also on the front-end security of customer accounts.

While this list is helpful, it is important to know that the adequacy of any given security measure will really depend on the specific business at issue and the facts of the matter at hand. So therefore, the best practice for implementing adequate and appropriate security measures will be to conduct a baseline risk assessment and then to develop measures based on the vulnerabilities or risks identified in that assessment.

Alan Kaplinsky:

Right. Right. So another question that concerns me a great deal, and I'd like to get your thoughts on this, Greg, is what does the CFPB's authority to do this, where does it come from? I always thought that only the FTC could deal with data security and safeguards. And so how does the CFPB come off as sticking its nose in this area?

Greg Szewczyk:

That's a great question, Alan. And it's a very controversial one. I mean, when the Dodd-Frank Act created the CFPB in 2010, it did not provide the CFPB with authority over data security. Instead, it was given a mandate to protect consumers from unfair, deceptive, and abusive acts or practices.

But the way I've seen it is back in 2015, the Third Circuit held in a case of FTC verse Wyndham that a company's failure to maintain reasonable security measures could amount to an unfair practice. And while that decision involved the FTC's authority under Section 5 of the FTC Act, the CFPB was paying attention. And the next year, we saw the CFPB bring its first action alleging that a failure to maintain sufficient data security standards fell within the proof. And in that case, I think it is important that there was somewhat of a difference between that and the circular, and that the CFPB specifically took issue with the statements that the company made about its transactions.

So this was a case involving Dwolla. And the specific complaints of the CFBP in that were that Dwolla had made statements to consumers saying that his transactions were safe and secure and saying that his data security practices exceeded industry standards and saying that it implemented some other specific data security measures, and that because it said that it used these and then didn't, that that created an unfair and deceptive act or practice. But I think that that's distinctly different from what we have in the circular that says the failure to maintain those acts and practices in and of itself is an unfair act.

So to get back to your point about how this is the FTC's turf. That has pretty much been what we've somewhat seen, the CFPB cede the authority over to the FTC, or at least not challenge its turf. And with this circular, depending on how they choose to enforce it and go forward, I think we likely would see some challenges to whether or not they actually have the authority to step in in this area.

Alan Kaplinsky:

And isn't there some express language in the Consumer Financial Protection Act, prior to Dodd-Frank that created the CFPB, which says that the CFPB doesn't have jurisdiction, or they can do things pertaining to Gramm-Leach-Bliley, I think, as I recall, but not dealing with data security?

Greg Szewczyk:

Yeah. You're absolutely right. So then I think we kind of get back into the West Virginia realm of if there is a challenge to this and if the argument is made that even though there is this express language, if in today's world that data security issues are considered an unfair act or practice, whether or not the authority was actually given there or whether you could interpret it in that way. And I don't want to try to read the tea leaves of how any challenge would go, especially because we don't know what the makeup of the Supreme Court would be when that challenge would be made, but there's certainly some vulnerability that the authority here does not exist.

Alan Kaplinsky:

Right. As I mentioned a little bit earlier, that's nothing new for the director of the CFPB. He's pushing envelopes every which way he can, including in addition to this something even maybe more controversial. He's determined that his UDAP authority, Unfair, Deceptive, and Abusive Acts and Practices, that that covers discrimination. Nobody has ever interpreted that UDAP authority as covering discrimination. And the FTC hasn't even concluded that it does under Section 5 of the FTC Act, which is the analog to the UDAP provision that the CFPB administers.

So let me ask you a question, Tim, and that is are there any precedents that companies can look to when trying to assess the adequacy of their data security measures and potential exposures?

Tim Dickens:

I think right in line with what you two were just mentioning, interestingly the circular focuses pretty heavily on some FTC cases in addition to those that Greg just mentioned. The first of those, okay, let's see, sorry. The first and most prominent of those actions was the one against Equifax following the reporting agency's 2017 data breach. This case really focused on the software update security measure that I had mentioned earlier.

In their complaint, the CFPB and FTC both alleged that Equifax violated the prohibition on unfair acts or practices by failing to patch a known vulnerability for more than four months resulting directly in a breach of personal information for over 100 million consumers. Essentially, where a business is aware of a particular vulnerability and does not take appropriate action to address the vulnerability, they would be unlikely to show that there are any countervailing benefits to consumers that outweigh the potential harms, and therefore there's likely CFPA liability, or there may be CFPA liability.

Another example looks directly at the FTC action against Qchex in 2006. In this, the FTC alleged that Qchex created and delivered checks without verifying that the person requesting the check was authorized to draw them on the associated bank account. Although Qchex implemented some procedures to verify the identity of its consumers and address this issue, it did not follow these procedures for all consumers, directly resulting in harms for Qchex customers.

The Qchex action highlights a failure to implement common sense practices including those that are required under the FTC safeguard rule specifically, which they addressed in the circular, is likely to result in liability. Essentially, it's not enough to simply draft policies and procedures, businesses must continuously oversee and monitor their conduct to ensure measures are actually implemented.

Alan Kaplinsky:

So Greg, let me ask you what are some concrete steps companies can take to mitigate the risk presented by the circular?

Greg Szewczyk:

At the very least, companies need to be considering implementing the specific controls identified in the circular. Regardless of whether there could be a challenge to the authority to actually enforce this type of a circular, there are specific controls listed there. They may not be sufficient, but they are at least necessary. And so companies need to be assessing whether multifactor authentication may be necessary or appropriate. They need to look at password management practices. And they need to update software and check for patch vulnerability whenever there is a new issue that has been announced.

Now, additionally, because the CFPB makes clear that following those measures alone may not meet the standard, companies need to think about how to tie their data security measures to recognize standards to build in some defenses. So you look to

not just the GLBA's updated safeguards rule, but you look to make sure that you're compliant with NIST or ISO or another industry standard where you can build in an argument that you have recognized adequate controls.

And almost equally important is kind of a general trend we've been seeing. The compliance needs to be documented in a way that matters to regulators. And what I mean by this is for a long time, infosec policies were really kind of technical documents written by technical personnel, delving into the specific ways that technical controls were implemented. And that makes sense. And while that technical side of it will never really go away because that's what we're talking about, the controls also need to be documented in more of a legal policy aimed towards their regulators.

So as companies update their policies to comply with, whether it's to comply with the circular or the updated safeguards rule or the 2023 privacy laws coming, they need to make sure that they're documenting those in a way that would speak to an attorney or a regulator or a judge or even a jury. Because you're not just positioning to put in place the technical measures, you're positioning to defend against challenges. And so you want to be speaking to your audience.

And as much as you don't want to think that data security is about justifying it to an attorney at the FTC, that is, or the CFPB, that's what we're talking about now. So we have been working with clients to make sure that they're positioning themselves that if they get a notice of non-compliance or if they get a subpoena, they're ready to comply with that in a way that shows their compliance in language that speaks to a non-technical individual.

Alan Kaplinsky:

So one final question, and then we'll have to wrap up today's show. But taking a step back, Greg, how do you see the FTC's announcement and the CFPB's circular in the bigger context of privacy and data security at the federal level?

Greg Szewczyk:

I think they both kind of epitomize what we've seen generally in the privacy regulatory world, and that privacy's a headline-grabbing issue and everybody wants to be relevant. It's politically advantageous on both the personal side for the people involved and the institutional levels to make sure that your institution remains important to be associated with new privacy initiatives. So it's not surprising to see agencies looking to be at the cutting edge. And I think we're going to keep seeing that.

But the flip side of that token is that companies can get caught off guard with a constantly changing landscape. It's hard enough to keep up with the state laws that keep changing, but then you see a new circular come up that might change immediately what your obligations are and it's costly and it's difficult to stay on top of everything that's changing.

So that's kind of the bigger picture context that we see it as. And one thing that we're advising companies is one way you can try to stay on top of this is not just be diligent and pay attention to what's going on, but pay attention and be diligent to what's going on on the state level as well. Because we often see, in the FTC context we've seen a lot of going hand in hand between say the FTC and the New York DFS with respect to cybersecurity regulations. That's something we've seen for years. What we're not sure how much we'll see is types of enforcement actions at the state level, whether those are going to drive similar enforcement actions at the federal level, say by the CFPB or the FTC.

And what I'm thinking about right now is we just recently saw the first enforcement action out of California's CCPA that's been in place for a couple years now. And that action focused almost entirely on analytics and also something called the global privacy control, which is a new mechanism that will allow consumers to essentially opt-out or block the collection of their analytics when they're going onto company's websites.

And there's a lot of issues with the GPC. It's a little outside of the scope of today. But those are the types of things that by staying on top of those and staying compliant, or at least off the radar of the state regulators, you may be able to stay off the radar of these federal regulators even as they keep on changing and morphing.

Alan Kaplinsky:

Okay. Well, I want to thank you, Greg, and thank you, Tim, for being on our program today. We covered a lot of area in a short period of time. And I hope our listeners enjoyed it. And I certainly want to thank them for taking the time to download our show today.

And I just want to remind all of our listeners that this is a weekly show and every Thursday morning we release a new podcast. And also want to encourage those of you that listen today to write a review of our podcast show if you got our show on a platform that calls for reviews. And if you have any suggestions for future podcast shows, please send them to us. You can send them directly to me at kaplinsky@ballardspahr.com. Thank you once again, and I hope everybody enjoys the rest of their day.