Consumer Finance Monitor (Season 7, Episode 52): Navigating the New CFPB Open Banking Rule

Speakers: Alan Kaplinsky, Greg Szewczyk, Hilary Lane, Alex Johnson, and Paige Paridon

Alan Kaplinsky:

Welcome to the award-winning Consumer Finance Monitor podcast where we explore important new developments in the world of consumer financial services and what they mean for your business, your customers, and the industry. This is a weekly show brought to you by the Consumer Financial Services Group at the Ballard Spahr Law Firm. And I'm your host, Alan Kaplinsky, former practice group leader for 25 years and now senior counsel of the Consumer Financial Services Group at Ballard Spahr, and I'm pleased to be moderating today's program.

For those of you who want even more information, don't forget about our blog, consumerfinancemonitor.com. It goes by the same name as our podcast show. We've hosted our blog since 2011, so there's a lot of relevant industry content there. We also regularly host webinars on subjects of interest to those in the industry. To subscribe to our blog or to get on the list for our webinars, please visit us at ballardspahr.com. And if you like our podcast, please let us know about it. Also, please let us know if you have any ideas for other topics that we should consider covering or speakers that we should consider inviting as guests on our show.

Today's show is a repurposing of a webinar that we produced on December 4th entitled Navigating the New CFPB Open Banking Rule: A Deep Dive. I'm going to introduce our speakers, and I'm going to start with Alex Johnson. For those of you that are active on LinkedIn and other social media, Alex Johnson will be no stranger to you at all. He is the founder of what's called Fintech Takes, a media brand that focuses on the intersection of banking, technology, and public policy. Alex has already written extensively about the rule that we're going to be talking about today, and I invite all of you to make sure you go on his blog, Fintech Takes, to read what he's have to say. Some of it he'll be talking about today. Alex has more than 20 years of experience in financial services with stops at Michael Mercado Advisory Group and Cornerstone Advisors.

Next person I want to introduce, a very special guest, Paige Paridon. Paige is Senior VP associate general counsel for Regulatory Affairs for the Bank Policy Institute. She is a member of the Bank Policy Institute's legal and regulatory affairs team and leads the consumer financial regulation advocacy and policy work. Prior to joining the Bank Policy Institute, Paige was managing director, senior associate general counsel of the Clearinghouse. And then prior to joining the Clearinghouse, Paige served as counsel in the legal division of the Board of Governors of the Federal Reserve System in the Banking Regulation and Policy Group. Very warm welcome to Paige and to Alex. You'll be hearing from Paige later in the program about the litigation that was initiated very soon after the regulation got published, which attacks the legitimacy of this regulation. She'll tell you what is in their complaint, or in their amended complaint, I believe, and where the lawsuit stands right now.

Let me finally introduce my colleagues from Ballard Spahr. Greg Szewczyk is a partner in our Denver and Boulder, Colorado offices. And he is the practice group leader of the Privacy and Data Security Group. And Hilary Lane is also a member of the Privacy and Data Security Group. We're very fortunate that Hilary recently joined us. She joined our firm during the past year. She focuses her practice very much on privacy and data security, providing pragmatic, strategic business savvy advice to help clients navigate the very complex global privacy landscape. Hilary previously served as the chief privacy officer at NBCUniversal. With all that out of the way, Greg, I'm turning the program over to you.

Greg Szewczyk:

Thanks, Alan, and thanks to everybody for joining us today. Before jumping into the substance, I just want to hit on the obvious fact that Alan has touched on already, which is when this rule was adopted, it was obviously under the last administration. The question before everybody is what is this rule going to look like under the next administration? Is it going

to be going forward in the same substance? Is it going to be going forward at all? And that's something that we're going to talk about later in the program, but there is a chance it could be repealed, it is a chance it could be going forward in a different form. There are different mechanisms that that could happen through. And those are important considerations as we go through this, but one thing that we do know is that companies can't just sit by idly right now and hope that the rule goes away. As most companies would already know that they've been considering how to structure their compliance for months at this point, so we're not starting from square one anyway.

What we need to do and what we have seen most of our clients do is to continue to consider how the final rules, how they have differed from the proposed rules, how the commentary informs how we should be interpreting these final rules, how that should be structuring what we should be looking at doing in the coming short term couple months, medium term, how the potential changes that could be coming through the new administration will be shaping what we're doing, and how those might be changed and what we could be doing could be leveraged on what we think those changes through the new administration would be, including some of the things that Alan talked about that will be addressed in future webinars in that series about what could be going on with state attorneys general. And so even if there are certain aspects that might be required for compliance with this rule, if the rule does not go into effect in that format, what steps might be taken now that could be leveraged down the road?

And so with that we're going to dive into the scope and the definitions. The first thing to address, to whom this rule would apply. The rule would govern two categories of covered persons, data providers and third parties. Data providers is defined to mean an institution under regulation E, card issuers under regulation Z, or any other person that controls or possesses information concerning a covered consumer financial product or service obtained from that person. We're talking about entities like banks, credit unions, and other providers of checking, savings, and credit card accounts and various other payment providers, or payment accounts and products. That third category would encompass a wide range of non-financial institutions including digital wallets, which is specifically discussed in the CFPB's examples.

And it's worth noting how much the commentary focuses on the intent behind digital wallets. And as with other rulemakings, the commentary spans hundreds of pages and often sheds significant light on how the current CFPB would interpret the rule. That's not to say that the next administration's CFPB would interpret it in the same way, but what we have seen with other rulemakings is true here where if you look at the rule on its face, the rule might be open to certain types of interpretations, but if you look at the commentary, it might be a more aggressive interpretation under the current CFPB and administration. And I think that that's particularly true when you look at how the CFPB issues the intent and the focus behind digital wallets. And its intent behind digital wallets really gives some insights into how it would interpret certain exclusions and certain other definitions. I think that's one important thing to keep in mind, as a general matter, go through and focus on how this rule would impact any given institution.

Taking a step back looking at it, if this would be a rule that would go into effect with the same current administration, the good news is that the rule would not apply across to the full scope of financial and products and services it could. The bad news is that this current CFPB has already stated that it would intend to implement the rule to many other covered entities through supplemental rulemaking. Again, we're put back in that flip-flopping position of what do we expect down the road? If the current rule survives or is revived under future administration, we now have a framework that could be revived and expanded beyond what this first final rule is. As I sit here and I think through how to apply this, we have a regulatory framework that could be adopted relatively quickly. And nothing is extremely quickly, but you have a regulatory framework that could be adapted and applied broader than what this first final rule is.

Moving on to the third party definition, it's defined to mean any person or entity that is not the consumer about whom the covered data pertains or the data provider that controls or possesses the consumer's covered data. A third party party could be another financial institution, that could be a data provider in its own right, but it would also include fintechs and data aggregators. And the rule has some special rules for data aggregators, which would be defined as an entity that is retained by and provides services to the authorized third party to enable access to covered data.

The next question on scope is what types of data will be impacted? The final rule applies to covered data in the data provider's control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider. Looking at covered data, first the rule defines covered data to encompass six categories of information. First, individual transaction information, two, account balance, third, information to initiate payment to or from a regulation E-

account which include any checking, savings, or similar account held primarily for personal family or account purposes, fourth, terms and conditions, fifth, upcoming bill information, and sixth, basic account verification information. The rule includes examples of data included in the first, fourth and fifth categories. And basic verification information is limited to name, address, email address, and the phone number associated with the covered consumer financial product service.

Notably in one of the most contested and commented on issues of the rule, the rule does not contain a specific carve-out for aggregated, anonymized, or de-identified data. One of the areas that it was considered for was in the context of covered data. We are going to address this more in the context of data use limitations, especially in the context of third parties, but this would've been a logical point where we could have included that type of an exemption. And it's an incredibly important one, especially in the fintech world, which is one of the main third parties, and an issue that was incredibly important.

And that's something that I'd like to bring up now to get ahead of it because I know later in the program is we always start running out of time as we always do. And Alex, I'd like to get your take because I know this is something that you've come up against is how big of an issue is it based on your reading of the commentary and your understanding in the industry of this decision not to include the exemption for de-identified, aggregate, and anonymized data as a carve-out from the definition of covered data?

Alex Johnson:

Yeah, this was a really interesting one. The commentary that industry provided to the CFPB on the rule really focused a lot on secondary data usage. And I think the main point that was made by industry was just that it's not fair to hold the open banking ecosystem to a standard that's significantly higher than the standards that exist in other areas where different versions of secondary use for data are permitted, particularly in the case of aggregate or de-identified data where the risk to the individual consumer of their data being misused is minimized. But the benefit to the companies is significant because you can develop risk models, you can use it for research and product development for new products. There are actual examples of companies in the open banking ecosystem that were built based on research and development that came out of aggregated or de-identified data that wouldn't have been possible under this new rule. The fact that that wasn't carved out in the final rule I think was surprising and disappointing to a lot of folks, particularly in the fintech ecosystem.

But in my conversations with Director Chopra at the CFPB, the intent or the reasoning behind keeping the secondary data use restrictions relatively tight was that in the absence of the US having a national data privacy law, his viewpoint, and I think the viewpoint of the CFPB, is that all new rulemaking that touches on consumers' personal data needs to hold itself to a higher standard in the absence of that other legal framework, and so I think that was the reasoning behind it. But certainly a blow to those who were hoping for a little bit more flexibility there in using de-identified data.

Greg Szewczyk:

Yeah, and one thing that I found a little interesting in the commentary, and I wish it had been addressed a little more directly is I understood and appreciated the points with the secondary use restrictions, and that was pretty consistent with what we see in state privacy laws, but in those state privacy laws, de-identified and aggregate and anonymized data is excluded from the definition of personal data if it fits within those definitions of de-identified and aggregate data. And so in that way, this goes beyond those state privacy laws.

And if we did have a national law, the bills that we have seen in Congress, regardless of how much of a chance they have really had to go anywhere, they have adopted that model as well. And so this still goes further than those. And I feel like there wasn't really that issue addressed of why it wasn't... The focus was really more on the secondary use as opposed to whether or not it should be incorporated into the definition of covered data itself, at least-

Alex Johnson:

Well, and I think one thing to just add onto that point is just this distinction that I think you're drawing, which is between potential for harm to consumers versus benefit to companies or to competition. And so I think the point that's really interesting here is it seems like in this particular case, the CFPB went a little bit above and beyond, to your point, where there's the potential for consumer harm. Because if it meets the requirements for aggregate or de-identified data, it really does

minimize any individual harm for the consumers. But it almost seemed more as if the Bureau was trying to not allow companies to get an advantage by having the data independent of whether it could cause harm to consumers. It did step a little beyond that privacy consideration, I think, to your point.

Greg Szewczyk:

Yeah, that's an excellent point. And turning to the scope of covered consumer financial product or services, the CFPB's rulemaking authority under Section 1033 extends to consumer financial products or services, which the CFPA defines to mean generally any financial product or service listed in the CFPA that is offered or provided for use by consumers primarily for personal, family, or household purposes. Listed financial products and services include a range of products and services provided to consumers including providing payments or other financial data processing products or services to a consumer by any technological means subject to limited exclusions.

Under the CFPA, the CFPB has the authority, including for purposes of section 1033, to identify additional financial products or services beyond those specifically listed in the CFPA. Relying on that authority, the rule would amend the CFPB's rules to include as a financial product or service providing financial data processing products or services by any technological means including processing, storing, aggregating, or transmitting financial or banking data alone or in connection with another product or service. The other product or service referred to in the last clause need not be financial as acknowledged by the CFPB. Although the CFPB believes the activities encompassed by this amendment are already within the scope of the activities listed in the CFPA, the codification is intended to provide even greater certainty. For purposes of the rule, the CFPB would initially limit the consumer financial products or services to the regulation E-accounts, reg Z credit cards, or facilitating payments from a reg E account or a reg Z credit card, excluding products or services that merely facilitate first party payments.

And with respect to that third provision, the final clause was added after the proposed rule was issued last year. And that was in part in relation to the commentary. But that may not be quite as broad as it seems. And this is another part where if you read the commentary, it may be interpretation that is influenced by the current CFPB and the current administration that could be subject to another interpretation under future CFPB directors and future administrations. It's one where we would definitely recommend that any individual company that's looking to avail itself of this particular exclusion really dig down into whether or not it falls within this exclusion, both under the current commentary and under whatever form of the rule may survive and go forward because it is very fact specific based on the type of marketplace; that may be and the type of transaction that's going forward. It's another area where if you are looking to take advantage of exclusions, you really need to go under not just the rule but also the commentary and what we see going forward.

And perhaps the biggest change from the proposed rule to the final rule, the CFPB extended the earliest compliance timeline. Under the proposed rule, the largest depository institutions would've had to comply within six months after publication while the smallest institutions would've had four years to comply. Under the final rule that was released a couple months ago, the largest depository institutions defined to mean those that hold at least $250 billion in total assets will have until April 1st of 2026 to comply. While this extended compliance date is obviously welcome news, the threshold for a company to fall within that category of the largest depository group was previously set at $500 billion in total assets, which means that more institutions will now be subject to the new initial deadline set forth in the final rule. Depository institutions with between $250 billion and $10 billion will have until April 1st of 2027. Those with between $10 billion and $3 billion will have until April 1st of 2028. Those with between $3 and $1.5 billion until April 1st of 2029, those with between $1.5 billion and $850 million will have until April 1st of 2030, and those with less than $850 million are exempt from the final rule entirely. And with that, I'll let Hilary take the lead to walk through data provider obligations.

Hilary Lane:

Access, what do we have to do? We have to provide access for authenticated customers and authenticated third parties including data aggregators to the most recently updated covered data. And that's an important point because that basically means that it's real time access. And this is going to be a heavy lift to be able to provide this, and it could be heavy volume once this comes into effect. The most recently updated covered data point is an important one.

It has to be an electronic form that's transferable to customers and third parties and usable in a separate system. Again, the format is important. And we'll talk a little bit about what that means for developers. No fee. You can't charge a fee for this

access so that the cost is on the institution. And again, there are two interfaces. There's the consumer interface and then the developer interface.

The developer interface, it's a standardized format and it has to comply with their performance standards and also interoperability requirements, meaning the requirements to allow the third parties to access and to integrate seamlessly with the system. There's a lot of undefined things, I think TBD by a standard setting body or bodies that will be recognized. But the standard is it has to be commercially reasonable, so it's either a qualified industry standard or a format that's widely used by developer interfaces of similarly situated providers and data. Again, the commercially reasonableness is dictated by either a minimum performance specifications or comparison that the QIS or comparison interfaces of similarly situated providers. And then there's security standards. First is you can't let the third parties use the consumer credentials for access. And also, it either has to comply with the GLBA, or if you're not subject to the GLBA, to the FTC's safeguards rule.

I talked about the standard setting body, and again, this has not yet been established, but there is some requirements or some attributes that the CFPB will look to in order to make sure that the standard setting body is fair, open, inclusive. Basically what that means is they want to be able to make sure diverse voices across all of the interested stakeholders are heard. It has to be open, meaning all interested parties can participate in the standard setting body. It has to be balanced. You can't have decision-making party concentrated in single interests. It has to include large and small institutions, and the decision-making power has to be balanced across all the interested parties. It is due process. Has to be publicly available, the process has to be publicly available, it has to be a fair and impartial process, and people have to know how does this work? Appealable, there has to be an opportunity to appeal it. And again, that also has to be open and it has to be clear, how that works has to be clear to the participants.

Consensus, it's what it sounds like. It's a general agreement. Doesn't have to be unanimous, but it does have to be fair and open, impartial and transparent process. And then transparency, knowing how do we participate? It's important for people to have the opportunity to participate, which means it's important for them to understand what they need to do to participate. And these are the things that the CFPB will look to to recognize the bodies that are established to establish these requirements for the industry.

Publication, it's another important part of the law. And again, it goes to the transparency of the rule. And institutions have to make the following information publicly available in both human and machine-readable formats. Again, back to the lift that's involved here. They're identifying information, legal and assumed name, a link to the website, contact information, developer interface documentation so the developers are able to integrate what do they need? It has to be made available in an easy to understand way. And again, the performance specifications. And that is the percent of requests in the preceding month for which a proper response was given. And the standard is 99.5%, which is a high standard. Again, it goes back to what is it going to take to comply with this rule?

And then written policies and procedures, the things that we've already talked about, the covered data availability. What are the data fields that are covered? And any exceptions that apply. And you can comply with this by incorporating the data fields defined in the QIS that we discussed earlier. Covered data accuracy and standardized format is a good idea for... And you have to address any reports of inaccuracy. And again, QIS can help with that. Record retention, again, this is largely about complying with the requests and responses. There's a three-year minimum retention for requests and responses and also a reasonable period of time for other evidence of compliance. Record retention, you have to keep a record of your compliance. And Greg, back to you, talk through the third-party obligations.

Greg Szewczyk:

Thanks, Hilary. We're going to move through these pretty quickly because I want to get to the last discussion and I also want to make sure that Paige has plenty of time to go through some issues on the lawsuit. In order for a third-party to access data, it has to satisfy the requirements to be an authorized third-party. And the rule implements a three-part authorization procedure for a third-party become that defined authorized third-party. Under those procedures, you have to provide the consumer with an authorized disclosure, certify that the third-party agrees to specific obligations, and obtain the consumer's expressed informed consent to access covered data on behalf of the consumer.

For the first prong, the third-party is required to provide the consumer with the authorization disclosure, whether electronically or in writing, is clear, conspicuous and separated from other material. That disclosure has to have the key terms

of access, and it has, among other things, the certification statement and a description of the third party's revocation mechanism, but it doesn't have to be required to take a particular form. The certification statement also needs to agree to specific obligations that are set forth in the rule. And we'll hit some of these with a little more specificity in a minute, but as you can see on the screen, they include certifying to the use of data only as reasonably necessary, duration and frequency, data accuracy, security revocation and fourth-party requirements.

And finally being authorized third-party, you must obtain expressed informed consent from the consumer electronically in writing to be authorized to receive the data. Alex and I talked a little bit when we were talking about that covered data about the reasonable necessity. And the requirement comes on that use by third parties of the limitation on use, and that is that third parties must limit the collection, use, and retention to what's reasonably necessary to provide the consumer's requested product or service. In a lot of ways, this is similar to what we've seen in state privacy law frameworks. We sometimes call this data minimization, we call it the prohibition on secondary use. It is a general push to try to make sure that data's only collected for either the purpose for its... For the collection of what is a stated purpose.

But the CFPB also took a slightly different approach than what is under state privacy laws, and we have seen that play out a little bit. Under state privacy laws, the secondary purpose is tied to the disclosed purpose of collection. Unlike that, the CFPB, its preamble to the proposed rules stated that it would treat the product or service as the core function that the consumer sought in the market and that accrues to the consumer's benefit. It had a slightly different focus for that as to how it defined what a secondary purpose would be.

And Alex, that's something that I wanted to ask you about is from what you had been hearing, you talked a little bit about the use that could accrue to the benefit of the third party or in the industry. Was that different focus of secondary use and how they tied it, is that something that you saw come through in comments that were submitted to the CFPB? Or is that kind of dichotomy more something that legal practitioners glamped on to and wasn't quite as big of an issue when it came to the actual practice?

Alex Johnson:

Yeah. No, I think the commentary that I saw, a lot of it was tied to benefit to the consumer. And so the argument was that even if this is not something that is directly reasonably necessary to the thing that they're getting today, if it is still for the benefit of the consumer, there should be some carve outs that allow for that to happen. And there were some accommodations made in the final rule that hint a little bit in that direction. For example, one of the exceptions that they included was the ability to use secondary data to prevent fraud. And so that's like a pro-consumer use case that is allowed and that was covered out even though it's not directly related to the actual product or service.

And so I do think there was pressure from the industry to loosen up these restrictions as long as it was aligned with the consumer, but, as you have outlined on the slide here, the challenge is from an industry perspective, a lot of times the way we define something that's beneficial to the consumer is more beneficial to us as the institution and arguably not as beneficial to the consumer. And I think that's where the CFPB was trying to draw more of a bright line. And that's things like advertising, cross-selling. Oh, you benefit because we're using your personal information to personalize your experience. I think that was where they drew the line, even though there is an argument to be made that it is to the benefit of the consumer.

Greg Szewczyk:

Yeah, I agree. I think those are obviously pretty clearly by rule cut off. I almost in some ways think that this is one of those weird situations where the commentary can be used by the next administration if this rule goes forward for companies to take a pretty aggressive stance. Because there's some commentary where they actually say that preventing fraud and improving the product aren't secondary uses but are within the beneficial purposes that the consumer's seeking. And while in some ways that's proceed at your own risk, it allows you to be somewhat aggressive in your interpretation. You might be more conservative under the current administration, but then next year you might feel a lot more comfortable taking a more aggressive interpretation that, say, training AI systems could be within. You could really kind of see how, depending on the administration and where you think the enforcement priorities are, you could get more aggressive and expand where that is with that language of just improving the requested product or service with that broad language.

Alex Johnson:

Yeah, just one quick point on that. About six months ago, I attended a speech that Director Chopra gave on the rule. And this was before the final rule was out, but he was providing some commentary and hints on where the final rule might land. And they asked him about secondary data and he said something to the effect, I'm paraphrasing here, of, "We're going to draw bright lines, and then it's up to adults to figure out what risks they want to take." And so it spoke to that same point of like we're going to build some level of I guess you could say ambiguity into the final rule, and then people are going to have to decide for themselves where they want to take risks. And I think you're absolutely right, that under a new administration and under a new CFPB, an update for more risk might make a lot of sense.

Greg Szewczyk:

The duration and frequency, you have to limit duration of collection to a maximum of one year. To collect beyond one year, you need to obtain a new authorization from the consumer. You can seek that reauthorization in a reasonable manner. Without that reauthorization, you can't collect covered data under the original authorization.

For data security purposes, we essentially see another type of expansion of the GLBA standards to systems that will collect, use, and retain covered data. Another question to Alex or anybody else on the panel is in a lot of ways we've seen the GLBA safeguards push through to fintechs through FTC actions, contracts and otherwise. How big of an expansion would this rule really be at this point as far as the imposition of the safeguards rule to the fintech community?

Alex Johnson:

Yeah, just one quick thought on that is that I have heard, and I don't know if this will happen now before we get a changeover to the next administration or if it's something that gets revisited under the next administration, but I have heard that there is a great desire on the part of banks and even regulators for more specific guidance around that translation of these risks into a third-party risk management framework. Because one of the points of tension that's come up a lot is all of these things that you're enabling are great, but it's not clear to banks how it translates into a third-party risk management context. And given everything that's already been happening in the banking as a service space, I think it's very reasonable for banks to wonder how does TPRM apply for data security or for other considerations to this whole new crop of third parties that you're forcing us to interact with? I don't know that I have a good answer to that, but I know that that's an area where there's been a lot of requests for additional guidance, and I suspect we might see some.

Greg Szewczyk:

Written policies and procedures, similar to what Hilary mentioned with data providers, there's a host of additional requirements on third parties. And again, we'll be providing the materials, as Alan mentioned at the beginning, we're just trying to move quickly for the sake of time. The rule also has specific requirements for data aggregators. As mentioned earlier, the authorization must disclose the name of the data aggregator and include a brief description of the services to be provided. Data aggregators must also certify to nearly all of the third-party authorization certificate requirements we looked at. And that applies even if the data aggregator is engaged after the third-party authorization.

Now, one thing I want to note that is not on the slide is just yesterday the CFPB proposed a new rule that would treat certain data aggregators as consumer reporting agencies under FICRA, requiring them to comply with accuracy requirements, provide consumer access to their information and maintain specific safeguards. That's beyond the scope of today. But it's notable that even on the way out, this current CFPB is still focused on this issue, and so it's something that we need to stay focused on. We've talked a lot about how this is an uncertain future right now, and so I want to make sure that we're giving enough time to Paige to get into a little bit about the lawsuit that she has going on, so I will turn it over to you.

Paige Paridon:

Sure. Thank you, everyone. BPI along with the Kentucky Bankers Association and Lexington Kentucky Bank challenge the CFPB's final rule the day it was issued, October 22nd. And then a couple of weeks ago, we filed an amended complaint adding some additional arbitrary and capricious claims to our complaint. Overall, our arguments rest on the fact that we're seriously

concerned that this rule is going to put consumers and their data in harm's way, particularly at a time when fraud is at an all time high.

And we note that importantly the statute does not provide the CFPB the authority to mandate the sharing of consumer financial data with third parties beyond entities that have a special fiduciary or other special relationship with consumers like agents or trustees, which is actually the language used in the statute. And so we argue that based on that statutory language as well as the intent, again, this statute was crafted as part of Dodd-Frank almost, well, 14 and a half years ago now. And this ecosystem that the CFPB claims to be furthering so-called open banking was not even on the radar for Congress at that time. The statutory language reflects the fact that that was not what Congress intended. The rule that the CFPB has promulgated expands their statutory purview impermissibly; that's our primary argument. But the arguments we make also about how the rule will furthermore harm consumers have to do with the fact that the rule requires banks to share sensitive consumer financial information including payment initiation data with third parties that the CFPB has not imposed robust data security requirements on, nor has the CFPB taken it upon itself to supervise these entities to ensure that they are complying with the minimum data security requirements that are provided for in the rule that were just discussed a few minutes ago with respect to GLEBA and the safeguards rule.

Furthermore, the CFPB does not take steps to ban a very insecure data sharing method, screen scraping. In fact, while the rule requires that data providers, which as formulated by the CFPB currently encompass primarily banks, while it mandates that they establish API secure developer interfaces is what the rule calls them, there's no requirement in the rule that third parties actually use these secure databases. And furthermore, the CFPB also in the final rule establishes a threshold above... or below which none of the requirements of the rule apply at all.

To the extent that the CFPB in the lengthy, lengthy preamble discussion talks about how important it is to sunset screen scraping, it hasn't taken any steps to actually do that. And so we have significant concerns that consumer data, including payment initiation data, is going to be mandated. Banks are essentially being mandated to share that data with third parties that may have less than robust data security protections. And so this information is going to be spread across potentially hundreds or thousands of fintechs or other third parties, and it will be ripe for the taking by scammers and fraudsters. And to the extent that fraudsters are able to obtain payment initiation information, they can drain consumers' accounts, and the consumer may not ever have any knowledge that their data has been compromised until it's too late and they've been victimized.

In addition, the CFPB provides relatively weak or what we believe are insufficient ability for banks, data providers to deny access to a third party based on risk management concerns. For example, if a bank has a concern that a third party that is seeking to obtain consumer data from a bank isn't going to protect the data sufficiently or has other concerns about some other aspect of their operations or compliance, the rule is not clear that the bank's risk management concerns would be respected. And the bank could potentially be subject to a CFPB enforcement action if it didn't provide access to that data.

It also doesn't hold appropriately third parties accountable for data breaches. Like I mentioned previously, there's no allocation or no effort to portion liability fairly within the system. The CFPB had been requested over many years that it had various stages of this rulemaking. That was a key aspect that the industry really needed some guidance and requirements of the CFPB in terms of liability, apportionment. And the CFPB failed to do that, which is concerning because it will allow third parties to... If they are breached or consumers are harmed, consumer has a right to come to the bank. And the bank of course is going to want to make the consumer whole, but there's no clear way or provision for the ecosystem as a whole to share in that liability in a way that's fair. And moreover, further to that point, there is a prohibition on banks or data providers from charging any fees to these third parties for obtaining the data or obtaining access to the interfaces to obtain that data.

And then we have concerns about the implementation timeline. As was discussed previously, there's are many provisions in the rule that are not clear how a data provider would comply with certain requirements related to data sharing. And the CFPB provides in many of those cases that a standard-setting organization that could be designated in the future, one or more could be designated in the future could potentially develop those compliance guidelines or requirements for data providers. And that abiding by whatever those requirements are could be in DISHA of compliance for a data provider. Well, first of all, we believe that that's impermissibly, arbitrarily vague and doesn't give data providers any real sense of how they can comply with the timeline.

And furthermore, to the extent that standard-setting organizations' development of these requirements is the only guidance provided to the industry, there have been no standard-setting organizations designated yet. But the timeline for compliance is

not to such designation or issuance of any standards by any standard-setting organization. In that way, the timeline appears to be arbitrary because it's set at least for the largest entities subject to the rule. The deadline is approximately 18 months from the final rule, but because there is no establishment of standards yet and unclear when that may happen, the establishment of a compliance deadline that's a date certain has been arbitrarily promulgated by the CFPB because data providers simply can't build towards compliance with unknown standards.

And we raise several other arbitrary and capricious arguments about the way that this rule could potentially put consumers in harm's way and the significant issues that consumers will have when this is allowed to explode potentially again without banks' ability to clearly limit access based on significant risk concerns. Banks are experts at managing risk. They manage risk for all manner of their operations, and they are subject to robust oversight by their potential regulators for managing risk, so they need to be able to have the discretion to determine whether it's safe and appropriate for them to share with these unvetted third parties that all of a sudden may be seeking all manner of sensitive consumer financial data of the bank's customers. That's an overview of the concerns that we've raised.

Greg Szewczyk:

Thanks, Paige. And I know you guys just filed that amended complaint relatively recently. Do you know off the top of your head any upcoming deadlines or when we can expect to see responsive pleadings? And last time I had checked, I don't think we had seen a responsive pleading by this yet.

Paige Paridon:

No, we haven't seen anything, anything yet. The deadline is in early January, I believe, for the CFPB to reply. Previewing the next topic here, the unknown elements, obviously there will be a change at the CFPB. Part of what we are kind of waiting to see and thinking through is whether and how anything changes at the CFPB with respect to this rule and then whether there's any knock on effects obviously for our concerns. And there very well may not be, but no response has been filed yet by this CFPB.

Greg Szewczyk:

Thank you. And that is a good segue into the next slide, which is the Congressional Review Act, which I think Alex, and then also we might be lucky enough to have Alan, who I know has a wealth of knowledge on this particular subject, I think we're going to walk us through how this may play out in the coming week, or coming month or so. Excuse me.

Alex Johnson:

Yeah. As a non-lawyer, I'll do the super quick version and then we'll call Alan off the bench to fill in all of the details. But for those who aren't familiar, the Congressional Review Act, which was passed in I think 1996, allows for Congress to review recently finalized regulatory rules and gives them a window of time. I think it's 60 congressional days to review, and then with a simple majority, essentially nullify recently passed rules. Interestingly in the, what, 30-ish years that this has been on the books, it was very rarely used prior to 2017. And then under the first Trump administration, it was used a lot to nullify rules that have been passed by the Obama administration. And so I think the speculation is that we'll see a similar usage of the Congressional Review Act either headed into the next administration or in the very early days of the next administration. But Alan, I know you probably have much more nuanced perspective on this. Do you want to jump in and add your two cents?

Alan Kaplinsky:

Well, thank you, Alex. Well, let me just add a couple of things because people may wonder how that 60 congressional days actually works. It doesn't mean calendar days; it's not even close to that. It's a much lengthier period of time. And I think as a rule of thumb, what I have heard is that any regulations that were promulgated by an agency, any federal agency, including of course the CFPB, after August 1 of this year are potentially subject to an override under the Congressional Review Act by the next Congress and the next president.

As you pointed out, during Trump 1.0, there were a host of regulations of the CFPB and other federal agencies which were overridden, including a regulation which was of great concern to me issued by the CFPB pertaining to arbitration provisions. And in that case, I was extremely happy that we were able to get that rule overturned.

The question of how that will be used in the next Congress with respect to this particular rule I think is very uncertain. For certain other rules issued by the CFPB that were finalized after August 1, I think it's much more likely that they may be overturned under the Congressional Review Act. If, for example, the CFPB were to issue a final regulation pertaining to overdraft fees, bank checking accounts, I'd say there's a very high likelihood that that could be overturned. The Democrats will oppose it. The Republicans, I think, will generally support that type of a regulation. And Rohit Chopra has not been bashful in terms of pushing the envelope, that is extending its jurisdiction into areas that are quite uncertain as to whether he has jurisdiction. And in those cases and in some other cases that we won't have time to go into today, but we'll deal with a lot on the three-part series of webinars that we're going to be doing.

The likelihood here, I think, is probably small because that'll be overruled. And principally, because whether you like or don't like this regulation doesn't really break down so clearly on partisan are you a Democrat? Are you a Republican? In this case, and I'm oversimplifying this, of course, but as Paige has so well described, the larger banks aren't thrilled about this rule, to put it mildly. On the other hand, the non-bank fintech companies that look at this as a business opportunity, they very much want the rule. They like the rule. And it is going to be, I think, a heavy lift to get this overruled under the Congressional Review Act. That's my own opinion. Do you share that, Alex?

Alex Johnson:

I do, yeah. I think that if you look at some of the on-the-record comments by members of Congress of both parties that are close to financial services or serve on the financial services committee, there's pretty broad bipartisan support I think for the idea of open banking. I would agree with you, I think it doesn't break down into as clear ideological lines as some other issues. I think it would be tricky.

Now, maybe this is a good segue to our next slide, but I think that that doesn't mean that there won't be political support for changes to the rule or even potentially repealing the entire rule and trying again with a different rule. Obviously, as Paige outlined before, the CFPB has not responded yet to the lawsuit. Unclear, from my perspective at least, if they will. But as she outlined, we are going to have a new CFPB director very likely. We are going to have a new administration and set of priorities for the CFPB. And obviously everything is on the table for that. Could be a repeal of the entire open banking rule, partial repeal of parts of the rule, or amended parts of the rule or significant changes to the scope of the rule.

Again, I think the point was made earlier, there was a lot of, I think, very well argued comments that were submitted during the comment period. The lawsuit from BPI outlined some very, I think, reasonable concerns from banks around the rule. And so I think all of that commentary could be the basis for some fairly significant changes to different parts of the rule. I will add my own plus one to one specific thing Paige said, which is it's extraordinarily difficult to prepare to be in compliance with a technical set of requirements when the specifications for those technical requirements are not finalized because we don't know what the standard setting body is. And that has not been officially designated.

And if you've been paying attention to the argument over standard setting and open banking, there are some pretty significant disagreements, I think, between the current CFPB and industry on what the right sort of composition is for a standard setting body. And I don't think either party feels like we're that close to being in full agreement there. I do think there are some areas where there are some pretty reasonable concerns that the next CFPB could significantly amend. I don't know if anyone else would like to add their two cents in on this one.

Alan Kaplinsky:

But let me, if I can add, something that I think it's not a big concern, what I'm about to describe is going to happen, but who knows falls into that category? And that is there have been a series of new arguments raised in a whole bunch of enforcement lawsuits brought by the CFPB that the CFPB has been unconstitutionally funded by the Federal Reserve Board since September 2022 when the Federal Reserve banks started losing money. The Dodd-Frank Act is very specific in saying that CFPB derives its funds from the Federal Reserve Board and it says from combined earnings of the Federal Reserve banks. And there's a large debate going on with a number of people in the industry saying earnings means profits. The CFPB thinks

that earnings means revenues. But that's all unresolved at this point. It's in active litigation; a lot of it in Texas. There's at least six lawsuits, probably more. And the issue could very well go up to the Supreme Court. We don't know what the new CFPB director is going to think about the lawsuit. It's a possibility that the Republicans could say, "This is an opportunity to get rid of CFPB entirely. Let's agree with the industry on this issue." I'm not saying that's going to happen, but I think there is a risk of that happening. That's the only thing I wanted to add, Alex.

Greg Szewczyk:

And Alan, that's a good segue into the concluding thoughts that we wanted to get to is where does this lead us in the future here? Which is everything's on the table. Apropos of what you just said, a couple of weeks ago the CFPB put out a report where one of its ultimate conclusions was that state privacy laws can and should regulate financial privacy and stop having carve-outs for financial information that's regulated by the GLBA, that that would not be preempted by it, which would be a pretty radical departure from how state privacy laws have operated to date. I ask the panel, and especially Hilary, where do you see things going? And especially with states having the general trend of expanding the types of data that have been covered by comprehensive state privacy laws, how do you see the trends for financial privacy going forward?

Hilary Lane:

I'll start. And I think we referenced that the CFPB has been post-election encouraging the states to take a look at where they can regulate the financial services organizations. And it will be interesting to see if they take them up on that. And as we all know, the state privacy laws vary in terms of what they already regulate, whether it's the GLBA exemption altogether or if it's just the GLBA data. It will be interesting to see if they take the invitation. We'll see. I think some probably will. Alan?

Alan Kaplinsky:

I don't have any further comments. Greg, do you have anything further that you want to say about the future, or Alex or Paige? If not, we will conclude our webinar. But yes, anybody have anything? If they do, speak up or forever hold your peace.

Greg Szewczyk:

I would just encourage everybody to join those three webinars that you referenced earlier. I think especially as we get into the new year, that third one is going to be particularly interesting as we hear more from... All three will be interesting, but I'm personally really looking forward as we hear more from the states as they unveil more on their plans of how they see their role in filling the gaps and we hear more details. I think that this is an area in particular where states are going to get more and more active. And I think it's going to be interesting to see how that plays out.

Alan Kaplinsky:

We saw that happen and Trump 1.0, Greg, and I think we're certainly going to see it happen in Trump 2.0. Well, with that, let me thank all of our speakers today, particularly our guests, Alex Johnson and Paige Paridon. And I also want to thank my colleagues, Greg Szewczyk and Hilary Lane. And even more important, I want to thank all of our many listeners who logged in today to hear what we have to share with you about this very new and very complex rule.

To make sure you don't miss our future episodes, subscribe to our show on your favorite podcast platform: Apple Podcasts, YouTube, Spotify, or wherever you listen. And don't forget to check out our blog, consumerfinancemonitor.com for daily insights on the consumer finance industry. And if you have any questions or suggestions for the show, please email us at podcast, that's singular, podcast@ballardspahr.com. And stay tuned each Thursday for a new episode of our show. Thank you very much for listening, and have a good day.