# Consumer Finance Monitor (Season 7, Episode 5): Navigating the Consumer Financial Protection Bureau's Proposed Personal Financial Data Rule

Speakers: Alan Kaplinsky, Greg Szewczyk, Ron Vaske, and Kristen Larson

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, the former practice group leader for 25 years, and now senior counsel of the Consumer Financial Services Group at Ballard Spahr, and I'll be moderating today's program. For those of you who want even more information. Don't forget about our blog, which also goes by the name of Consumer Finance Monitor. We've hosted our blog since July of 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. So 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 that. You can leave us a review on whatever platform you're utilizing to access our podcast show. Also, please let us know if you have ideas for other topics that we should cover on our podcast show or speakers that we should consider inviting as guests for our show. And I'm very pleased to let our listeners know today that very recently our podcast show was ranked by Good2bSocial as the best podcast among law firm podcast shows in the United States devoted exclusively to consumer financial services. Good2bSocial is a prominent law firm consultant owned by best lawyers, and we're very gratified by this recognition from one of the country's leading social media consultants for law firms. Today our podcast show is a repurposing of a webinar that we did on December 18th entitled Navigating the Future: Understanding the CFPB's Proposed Personal Financial Data Rule.

Let me just give you a little bit of background about our webinar today. We're going to be delving pretty deeply into the CFPB's proposal dealing with personal financial data. This comprehensive discussion that we're going to have today will explore the implications and the intricacies of the proposed rule, addressing its potential impact on consumer privacy, data security, and financial services. Our panel will dissect the key provisions, regulatory framework and potential challenges equipping you with the knowledge that you need to navigate this evolving landscape dealing with personal financial data regulation.

So let me introduce to you our speakers for today. First of all is Greg Szewczyk. Greg is a partner in our Denver and Boulder, Colorado offices and he's a practice co-leader of the Privacy and Data Security Group. He's a lawyer who's leveraged over a decade of experience in high stakes litigation to help companies assess risk and to comply with an ever expanding patchwork of federal, state, and international privacy and data security statutes and regulations.

Next to Greg is Ron Vaske. Ron co-leads our FinTech and payment solutions team. His practice focuses on matters involving banking, payment systems, and commercial transactions. Ron regularly assists clients in relationships between financial institutions and fintechs or other third parties. He has more than two decades of experience helping clients establish and administer bank sponsorship arrangements for credit card payment systems, innovative technology, information security operations, and customers experience and servicing.

And last but not least is Kristen Larson who after having had more than two decades of experience working for two different large banks, large regional banks in the consumer financial services regulatory area, which includes privacy and data security, joined us about a couple of years ago to augment our practice in the consumer finance area.

The agenda for today, let me just tell you who's going to be covering what. Rulemaking background. In just a moment, I'm going to turn it over to Kristen who will cover that topic. And then I will go to Greg. And by the way, I apologize for mispronouncing Greg's name, it's Szewczyk, I got it wrong the first time. Greg will talk about the proposed rule and then talk about the impact on privacy, impact on data security. Then we will go to Ron who will talk about the impact of financial

services. And finally, Ron is going to talk about a somewhat related CFPB advisory opinion issued under Section 1034 of Dodd-Frank, that has in and of itself become quite controversial. So with that introduction, it's my pleasure to turn the program over to Kristen.

Kristen Larson:

Thank you, Alan. Happy to be here today. I'm going to provide a brief overview of the rulemaking on open banking. As Alan had mentioned, there has been substantial background in the rulemaking that started back in 2016. And most recently in 2023, the CFPB had issued market monitoring orders looking to get information from data aggregators related to contracts, payments, data security, error resolution, liability, fraud, data, accuracy, customer controls, and privacy uses of data, metric, and traffic. And then for data providers, they were looking at receiving information related to consumer's direct access, screen scraping, third-party portals and third-party service providers. Additionally, as a part of this process, the CFPB also published outlines and followed the requirements for their SBREFA obligations and published their report related to that in April of this year.

And so the more important part that they started with was their advanced notice of proposed rulemaking, which was three years prior to when they came out with the proposed rule. Essentially, the Bureau is required to engage in this rulemaking. And as a part of the rulemaking, they're supposed to consult with the other credential regulators, the Fed, the OCC, FDIC, and FTC to ensure that the rule is imposing substantially similar requirements on covered persons, that it takes into consideration certain account conditions under which the covered persons do business in the US and other countries and doesn't require or promote the use of particular technology in order to develop the compliance system.

The next part that I wanted to address briefly is the financial trade groups had petitioned the CFPB prior to this proposed rulemaking to ensure that the data aggregation services were fair, transparent, and competitive. Essentially, they were concerned that the rules that the financial institutions have to meet are very stringent and that the other players in the markets did not have some of the same requirements. And so they're looking and urging the CFPB to define these rules and level out the playing field for some of the other participants. Their concerns is that there's all these additional people that are collecting, storing, and selling consumer information that don't have the same standards that the financial institutions are subject to and aren't being supervised, which is putting the consumers and their financial information at risk.

And with that, I'm going to turn it over to Greg to talk about the proposed rule that came out in October.

Greg Szewczyk:

Thanks Kristen, and thanks for everybody for tuning in today. There's a lot to unpack on the rule itself, and we're going to do our best to hit the most relevant issues, but just due to time, we're not going to be able to hit everything. At the 10,000-foot level, the proposed rule provides new rights and imposes new obligations related to certain types of consumer financial data. This includes a right of access for consumers and third parties, and that right also has a data portability component. It also requires that such access be accomplished through interfaces designed to move the industry away from screen scraping. And the rule would also impose what would be pretty significant limits on how third parties can use data.

With the exact impact still somewhat up in the air as the CFPB's preamble and explanation has requested some comments on specific issues because they know that this would have a big impact on some common practices. The proposed rule would also expand the scope of data security regulations, especially the GLBA's Safeguards Rule, which as most know was updated earlier this year. And so that's obviously a pretty broad spectrum and with some pretty significant impacts on several fronts. So we're just going to dive right into the specifics.

The first thing to address, to whom this proposed rule would apply. And the rule would govern two categories of covered persons, data providers, and third parties. Data providers is defined to mean an institution under Regs E, card issuers under Reg Z or any other person that controls or possesses information concerning a covered consumer financial product or service obtained from that person. So we're talking about entities like banks, credit unions, and other providers of checking, savings, and credit card accounts, and various other payment accounts and products. But that third category would encompass a wide range of non-financial institutions such as digital wallets, which was an issue specifically discussed by the CFPB in the preamble and in its commentary. The proposed rule would have a limited exception for depository institutions that do not have a consumer interface.

So the good news is that the current proposed rule does not apply to the full scope of financial products and services that it could like mortgage, automobile, and student loan payment accounts. The bad news is that the CFPB has stated that it intends to implement the rule to those other covered entities through supplemental rulemaking. So even if your entity is not going to be within the scope of 1033 immediately, you do still have an vested interest in how this develops. Third party is 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. So a third 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 proposed 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 cover data.

The next question on scope is what type of data will be impacted? The proposed rule would apply 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. So the two big issues there are the definition of covered data and the definition of covered consumer financial product or service. Looking at covered data first, the proposed rule would define covered data to encompass six categories of information. Individual transaction information, both pending and historical. Account balance. Information to initiate payment to or from a Reg E account, which would include any checking, savings, or similar account held primarily for personal, family, or household purposes. The terms and conditions that apply. Upcoming bill information. And basic account verification information.

The proposed rule would include examples of data included in all but the second and final categories, account balance and basic account verification information. For that latter category, the data provider's obligation would be limited to providing the name, address, email address, and phone number associated with the covered consumer financial product or service. Notably, the proposed rule does not carve out or exempt aggregated, anonymized, or de-identified data. So with the broad definitions of those covered data subsets, that data derived from those subsets would constitute covered data.

The CFPB seems to understand just how important that issue would be as it's specifically requested whether de-identified data should be carved out in some fashion. And we'll talk about how this comes into play later, but given how prevalent the use of de-identified and aggregate data is by third parties like fintechs for various purposes, we can be confident that the CFPB is receiving ample comments on that front. But in any event, in complying with this obligation to provide covered data, a data provider would need to make available the most recently updated covered data that it has in its control or possession at the time of the request, including information concerning authorized but not yet settled debit card transactions.

Turning to the scope of covered consumer financial products 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 payment or other financial data processing products or services to a consumer by any technological means subject to some 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 proposed 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 combination with another product or service.

The another product or service referred to in that last clause need not be financial as acknowledged by the CFPB in the preamble to the proposed rule. Although the CFPB believes that the activities encompassed by this amendment are already within the scope of activities listed in the CFPA, the codification would be intended to provide even greater certainty on the issue and to provide additional assurance that financial data processing by third parties or others is subject to the CFPA and its prohibition on unfair, deceptive, and abusive acts or practices.

For purposes of the proposed rule, the CFPB would initially limit the consumer financial products or services about which data providers must provide data to those that are covered consumer financial products or services, which is defined to mean Reg E accounts, Reg Z credit cards, or accounts to facilitate payments from a Reg E account or a Reg Z credit card. That third category is intended to clarify that the proposed rule would cover all consumer-facing entities involved in facilitating the

transactions the CFPB intends to cover. As I noted earlier, the CFPB states in the preamble that it intends to implement these Section 1033 requirements with respect to other payments and payment accounts related to products through supplemental rulemaking. So even though this is a somewhat limited account right now, it's signaling where we're going in potentially the near or at least medium term.

Moving on to the obligation that 1033 would impose, we'll start with data providers and the first obligation relates to data access. Under 1033, data providers would need to provide access for authenticated consumers and authenticated third parties to the most recently updated covered data. That data would need to be in an electronic form that is transferable and usable in a separate system. The purpose of the data portability requirement is to facilitate the ability of consumers to switch financial institutions more easily, and that's a mandate that came directly from President Biden and the White House throughout the past couple of years. Or as the CFPB puts it, the purpose is to jumpstart competition by permitting consumers to direct existing providers to share data with other companies offering better products and enabling consumers to walk away from bad service.

In any event, the access and portability rights would essentially extend the privacy rights afforded under the now 13 states that have privacy laws on the books to subject financial institutions. As all of the privacy laws exempt either GLBA-regulated entities entirely, or MPI regulated by the GLBA, this is a significant expansion. Data providers would be prohibited from charging a fee on consumers or third parties for accessing covered data, and the process would need to be done through two interfaces, one for consumers and one for third parties. The consumer interface could be done through existing practices such as online banking or mobile apps. So while there might be some changes to update, it really does fall within an existing framework that we already have. But the developer interface would mark a significant change from current practices. Ron will talk about the operational impact more later, but essentially the new requirement is designed to end the common practice of screen scraping.

So let's take a look at the proposed rules obligations relating to that new developer interface. The developer interface would be defined to mean an interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable by authorized third parties in response to the request. So again, we're talking about other financial institutions, fintechs, data aggregators, and similar third parties. Developer interfaces would be required to satisfy several additional requirements related to format, performance, and security. With respect to the standardized format, an interface would be deemed to satisfy this requirement if it makes covered data available in a format set forth in a qualified industry standard, or in the absence of such a standard in a format that is widely used by the developer interfaces of other similarly situated data providers with respect to similar data and is readily usable by authorized third parties.

We'll go into what a qualified industry standard means and how that's defined in a moment. But for now, it's worth noting that this is the one instance in which adherence to a qualified industry standard would provide a full safe harbor and not merely constitute indicia of compliance with the relevant requirement of the proposed rule. And with respect to the performance standards, a data provider's developer interface would be required to perform at a commercially reasonable level. Commercial reasonableness would be dictated by quantitative minimum performance specifications and additional specific indicia of commercial reasonableness.

Subject to certain exclusions and conditions, the quantitative minimum performance specification would be a response rate of at least 99.5%. The proposed rule would define response rate in certain related terms, including what qualifies as a proper response and a commercially reasonable amount of time to provide a response, which as it currently sits, would be no more than 3500 milliseconds. Indicia of performing at a commercially reasonable level would include, first, whether the performance of the interface meets the applicable performance specifications that would be set forth in the QIS, and whether the performance meets the applicable performance specifications achieved by developer interfaces established and maintained by similarly situated data providers. So again, we're seeing the comparison to the QIS and also to other similarly situated data providers.

And finally, data providers would be required to implement several data security features in their consumer and developer interfaces. In a provision aimed at eliminating screen scraping data providers would be prohibited from allowing a third party to access the data provider's interface by using any credentials that a consumer uses to access the consumer interface. In addition, data providers would be required to apply to their developer interfaces a data security program that satisfies the requirements of rules issued in furtherance of GLBA Section 501, which we frequently refer to as the Safeguards Framework.

And that specific framework will depend on the regulator of its state, but for data providers not subject to section 501, it would be required to apply the information security program set by the FTC Safeguard Rules.

So with the safe harbor and indicia provided to the qualified industry standards, it's worth taking a quick look at how those are defined. Now, the proposed rule would define qualified industry standard to mean a standard issued by a standard setting body that is fair, open, and inclusive in accordance with the criteria specified in the rule. Under the proposed rule this would occur when the body has all of the following. Openness, meaning the sources, procedures, and processes used are open to all interested parties, including data providers, authorized third parties, data aggregators, relevant trade groups, and consumers and other public interest groups. Balance, meaning the decision-making power is balanced across these interested parties. Due process, so the use of documented and publicly available policies and procedures, adequate notice of meetings and standards development, sufficient time to review drafts, access to participant views, and fair and partial conflict resolution.

An impartial appeals process, a requirement that the standards are developed through consensus. Transparency, so that the procedures and processes for participating in standards development and for developing standards are transparent to participants and the public. And recognition by the CFPB within the last three years as an issuer of qualified industry standards. Now, the proposed rule would also permit the standard setting body to seek the CFPB's recognition as an issuer of QIS. And we'll see the QIS come into play with third parties as well. Another obligation for data providers relates to publication. Under the proposed rules, data providers would need to make certain information publicly available in both human and machine-readable formats. Under the rule, this would be required information to be made in a readily-identifiable format to members of the public, meaning at least as available as it would be on a public website.

The specific information that must be disclosed would include identifying information, the developer interface documentation, and performance specifications. On identifying information, we're talking about the legal name, and if applicable, any assumed name the company is using when it's doing business with the customer. A link to its website, its Legal Entity Identifier, and contact information that would enable a consumer or third party to receive answers to questions about accessing data. On the interface and performance issues, the data provider would be required to publish documentation including metadata describing all covered data and their corresponding data fields, sufficient for a third party to access and use this developer interface. The published information would need to be maintained and updated as the interface is updated, include how third parties can get technical support and report issues, and be easy to understand and use.

The data provider would also be required to publish on or before the 10th calendar day of each month the percent of requests for covered data received by its developer interface in the preceding calendar month for which the interface provided a proper response. These go beyond what's just in periodic privacy policy updates and include some pretty significant burdens there. Data providers will also be required to maintain written policies and procedures related to covered data availability and accuracy, and maintain records relating to its requests and responses. Qualified industry standards can be used as an indicia of compliance on these requirements, but they're not safe harbors. There are more specifics on these issues, but since we still have a lot to cover and limited time today, I'm going to keep moving forward.

Turning into the obligations for third parties. In order for a third party to access data, it has to satisfy the requirements to be an authorized third party. The proposed rule would implement a three-part authorization procedure for a third party to become an authorized third party. Under those procedures, the third party would be required to first provide the consumer with an authorization disclosure. Second, certify the third party agrees to specific obligations. And third, obtain the consumer's expressed informed consent to access covered data on behalf of the consumer.

On that first prong, the third party would be required to provide the consumer with an authorization disclosure, either electronically or in writing. It's clear, conspicuous, and segregated from other material so it cannot just be buried within a standard set of terms. Now, the authorization disclosure would be required to include the key terms of access set forth in the proposed rule, including the certification statement and a description of the third party's revocation mechanism so that consumers are able to revoke consent from the third party. The authorization disclosure would also need to include the name of any data aggregators that would be assisting the third party with accessing covered data and a brief description of the services the data aggregator would provide.

The certification statement would need to agree to the specific obligations set forth in the proposed rule. We're going to hit on some of these with more specificity in a minute, but as you can see on the screen, they include certifying to using the data only as is reasonably necessary, practices related to data accuracy and security, providing a revocation method so that the

consumers can revoke consent, and requirements that must be pushed down to fourth parties. And finally, to be an authorized third party, the third party must obtain the express, informed consent from the consumer electronically or in writing to be authorized to receive that data.

We don't have time to go into all of the obligations. There are a few worth looking at with a little more detail, the first of which is the reasonable necessity requirement. Now, under this requirement, the third party would need to limit collection, use, and retention of covered data to what's reasonably necessary to provide the consumer's requested product or service. According to the CFPB's preamble, the reasonably necessary standard is similar to standards and several data privacy frameworks that minimize third party's collection use and retention of data. But unlike for state privacy laws where the prohibition on secondary use is tied to the disclosures at the point of collection, the CFPB will treat the product or service as the core function that the consumer sought in the market and that accrues the consumer's benefit.

So under the current rule, it's not clear that companies would be able to use covered data whether in full or in aggregate or in de-identified form to improve its own internal operations, even though that could arguably be accruing to the consumer's benefit. The proposed rule would also identify targeted advertising, cross-selling of other products or services, and the sale of covered data is not part of or reasonably necessary to provide any other product or services. So third parties would be able to engage in those activities only to the extent the consumer sought to obtain them as, quote, "A standalone product."

The CFPB has specifically requested comments on these issues including whether there should be different opt-in requirements for some types of secondary uses, such as improving products or operations versus targeted ads and sales. Now, the CFPB has also asked for comments on whether the use of de-identified data should be carved out from this requirement, either generally or with some level of specificity. Comments aren't due until December 29th, so we don't have a lot of industry comments yet, but we do understand that there is going to be ample comments coming in on this particular issue. I know that there's not a whole lot of time between December 29th and now, but if this is an issue that's going to be impacting your company, it may be worth considering whether it's worth trying to get a comment in by that December 29th deadline as this could be an issue that has very significant impacts.

Turning to the duration frequency requirement, the third party would need to limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent reauthorization. To collect cover data beyond that period the third party would need to obtain a new authorization from the consumer no later than the anniversary of the most recent authorization. The third party would be permitted to seek reauthorization in a, quote, "Reasonable manner" with indicia of reasonableness, including conforming to a QIS. If the consumer does not provide a new authorization before the one-year period ends, and even if the consumer has not affirmatively revoked the authorization, the third party would no longer be able to collect new covered data pursuant to the most recent authorization or use or retain covered data that was previously collected pursuant to the then accurate authorization, unless the use or retention of that covered data remains reasonably necessary to provide the consumer's requested product or service.

The proposed rule would include examples of what reasonably necessary uses means such as uses specifically required under other provisions of law, including complying with subpoenas, protecting against fraud, and servicing or processing the product the consumer requested. The preamble states that the reasonable necessity would also include whether is a clear and affirmative indication by the consumer that they want to continue the use of the product beyond the maximum period in a manner supported by the use and retention of data collected prior to the expiration of that period. So even though that retention requirement could have big impacts, there is still some indication that there's a practicality being considered.

With respect to data security, we saw earlier that the imposing of the GLBA Safeguards Framework to data providers with respect to the developer interface. For third parties, those standards would apply to the systems that will collect, use, and retain covered data. Now, in other words, the Safeguards requirements will be imposed much more generally on third parties. Now, some third parties such as many fintechs have denied or expressed uncertainty as to whether they are financial institutions within the mean of the GLBA and the FTC Safeguards Rule. So for these third parties, the CFPB approach would require compliance with those Safeguards Rules even if the third party doesn't consider itself subject to the GLBA.

Now, there are some enforcement questions here, but it certainly marks a pretty big expansion of those requirements. As with data providers, the proposed rule would require third parties to implement various written policies and procedures. The third parties would have flexibility to determine its policies and procedures in light of their size, nature, and the complexity of its activities. But certain specified records would be required, namely the signed authorization disclosure and a record of actions

taken by the consumer to revoke the third party's authorization, as well as any data aggregator certification statements provided to consumer. Now, a third party would be required to periodically review these procedures and update as appropriate. And it's also worth noting that the FTC Safeguards Rule requires that certain policies be in writing. If the Safeguards Rule would be a new requirement for a third party, there are additional written policy requirements beyond what is in the proposed rule.

The proposed rule has some specific requirements for data aggregators. We've mentioned the middle one there already about disclosing the name and a brief description of the services, but the data aggregator could also perform the third party authorization on behalf of the third party for which they work, but the liability would still ultimately run to that third party. The data aggregators must also certify to nearly all of the third party authorization certificate requirements that we looked at a minute ago, and that applies even if the data aggregators engage after the third party authorization has already been made.

I'm going to move through these next slides very quickly because we still have a lot to get through today, but there are some exceptions to the rule, both related to the nature of the data and the interface. Looking at the exceptions related to the nature of the data, the proposed rule would include four categories of covered data that a data provider would not be required to make available to the consumer or authorized third parties. And that includes confidential commercial information, including an algorithm used to derive credit score or other risk scores or predictors, information collected by a data provider for the sole purpose of preventing fraud or money laundering, or detecting or marking any report regarding other unlawful or potentially unlawful conduct. Information required to be kept confidential by any other provision of law. And information that a data provider cannot retrieve in the ordinary course of its business with respect to that information.

Notably, the CFPB's preamble makes it very clear that these four exemptions are intended to be narrow, and there's some specific stuff related especially to that second category about whether or not information is collected for a sole purpose. And the CFPB has said that it intends to monitor the market for pretextual uses of these exemptions.

The proposed rule would also include several circumstances tied to interface access in which a data provider would not be required to make covered data available to the consumer or an authorized third party. These exceptions include the insufficiency of information related to authentication, the data request or the third party, and they also include risk management and availability issues. There's a lot to unpack for each of these that we don't have the time to do, but it's worth noting that denials of access related to risk management, insufficient evidence regarding the adequacy of a third party's data security practices, or a third party's failure to make public specified information about itself would be subject to a reasonableness standard, meaning that access could not be denied if the denial is unreasonable, even if that exception appears to apply.

And the last thing we're going to talk about about the rule itself is the compliance timeline. As you can see on the screen, the proposed rules will be tied to the size of the covered entity. Thresholds are pretty straightforward, so I'll just note that for the largest companies that compliance deadline is very quick, just six months after the publication of the final rule. And we expect to see pushes in the comments for extending the implementation deadline. But it's a reminder that this may not be one of those situations where companies can really wait and see how the final rule is published because there are some serious operational changes that need to be made, especially with respect to developing that interface.

So very quickly, just some notes on takeaways, most of which we've already discussed. On the privacy front, the rule would obviously expand privacy rights into this field in a pretty significant manner. And even for entities that are already affording the rights to a subject, many are doing subject to a fee and that's going to need to change. The limitations on use by third parties is another obvious big picture impact, especially if these of de-identified information remains curtailed. Now, it could have some big impacts on the improvement of products, and it also could cause many companies to have to go and rework their algorithms and the way that their products worked because they're designed to run off of that de-identified and aggregated information. And finally, more notices and consents. I know a lot of clients feel like they're constantly battling changing laws and regulations to provide the proper disclosures and the proposed rule would just add to that. The data provider publication requirements would require very frequent updating, meaning more hours and resources devoted to this issue.

On the data security side of things, the expansion of the GLBA Safeguards Rule could mark a pretty significant obligation for many third parties that have not considered themselves subject to the rule. Especially with the update that went into effect earlier this year, that can mean some pretty big operational changes related to things like encryption at rest, and MFA anytime

someone's accessing this information. Or relatedly, more requirements for written policies and procedures, that may not be as big of an issue for more established entities, but for some of those smaller companies in the field, it could be a barrier to entry entirely without the necessary funding or resources. It also introduces more paper to review during diligence of business partners, whether it's in the context of developing contracts with third parties or in the M&A context.

And finally, there's going to be more sensitive data in portable format. Now, there are these data security requirements about that, but anytime you have sensitive data in a portable format, that can obviously increase security risks and we could have disputes over which entity would be held accountable for data breaches because that's not really addressed in 1033. I know I just talked to you pretty quickly for a lot. Again, I'm happy to speak offline on specific questions, but with that, I'll turn it over to Ron for some more analysis on how the proposed rule would impact companies from an operational standpoint.

Ron Vaske:

Thanks, Greg. We'll get right into that. After hearing what Greg had to say in his presentation, I think it should come as no surprise that the impact on financial companies is going to be significant. Some of the benefits probably, things that certainly any data provider would see as a benefit is a move away from screen scraping and all of the bad things that come with that, the liability to the financial institution. As well as granting access or having the third party get access to more information than they really need to provide the service that they're going to provide to the consumer. It will establish more transparent standards for consumers, for banks and non-banks. That's helpful. One of the things that I think data providers would not like, obviously there would be a lack of stickiness in accounts. With consumers having more control over their data and ability to give it to someone else, they're definitely going to have more ability to move from one financial institution to the other. So losing some stickiness there.

Also, something to think about, whenever there's a new rule like this that the federal government comes out with, usually expect states to come in with their own. And usually they're going to offer or they're going to provide even stronger protections than what it's provided under the federal regime. So watch for that.

Okay, some more on impact to financial companies. Obviously, significant costs would be expected here to implement system changes and to create data sharing processes. If the rule is enacted as proposed, you'll need to take a deep dive and review, and where necessary, revise your consumer documentation, your data compliance policies, all of your disclosures, and even commercial agreements that you may have with third parties that deal with this data. Prepare to establish and maintain systems that can receive data access revocation requests, track duration-limited authorizations, and delete data when required due to revoked authorizations, lapsed authorizations, or because retaining the data is no longer reasonably necessary.

Probably no surprise that there's a lot of pushback from industry here at least seeking additional comment time. Typically, the CFPB provides 90 days for comments and particularly on significant rulemaking like this. This rule I think it's around 70 days that it's being offered, and there's a lot of complexity here and a lot to get through. Probably warrants additional time. In particular, this is during the November and December holiday season where companies aren't necessarily as able to respond to a lot of things going on. Small business entities who could be disadvantaged by the requirement need additional time due to their limited resources, and additional time is needed for industry to understand how the rulemaking intersects with the upcoming Reg V rulemaking, the FCRA rulemaking that's probably going to be intersecting. So with that, I will turn it over to Kristen who will give us some information about Section 1034(C), advisory opinion. Kristen?

Kristen Larson:

Thanks, Ron. We wanted to touch a little bit on the CFPB's advisory opinion on Section 1034(C) as it relates to the same types of issue of providing information to consumers requests. The CFPB came out with an advisory opinion shortly before the proposed rule, and they essentially said, "We're issuing this guidance to halt large banks from charging illegal junk fees for basic customer service." And so what their concern is, is that large banks and credit unions had been charging consumers a fee or charge to request some basic types of account information that they were entitled to already.

And with that, they stated, "Under the Section 1034(C), consumers have a right to this information, that there's a legal obligation on the large banks and credit unions to provide this information." And it does not require the large banks and credit unions to provide the information in any particular means, similar to 1033, that says you have to make it available in electronic form. Here, if you had paper records or electronic records, you could share with the consumer in that same format of giving

them paper copies. It's prohibiting you from imposing conditions or requirements on the request that would unreasonably impede their access to the information.

And then on top of it, an unreasonable impediment of course, is charging fees to respond to their inquiries for information on their deposit accounts, on their loan accounts, getting specific types of supporting information, be it their original account opening agreement, the check image. Or charging them for some of the research that you'd spend on gathering that information.

The other things that they talked about is other types of impediments that are not fee related, would be having the consumers have an excessive wait time to make a request, whether that's calling into a call center where they have to wait a long time before they can talk to someone who can help them, requiring them to submit the same request multiple times. They also, as we previously know from their June guidance, they don't like having consumers have to respond to a chat box where depending on what they say, it may take a long time for you to get to the right person to request the information that you want or saying, "We have that information, but you need to go to this third party to access this information." They don't want you to be pushing consumers to a third-party service provider.

Then one of the other things that they said in the advisory opinion that they expect timely delivery. They expect that the information will be accurate and complete. They're looking for you to be responsive to the extent that the information is in the controller possession, and if you're providing incomplete and inaccurate information that you're really not being responsive. So for example, a consumer says, "Give me five years worth of account statements," you can't just provide the last year and pretend that you've satisfied the request. The CFPB would find that to be a violation. Or if the consumer was asking for information about the cost of doing some sort of transaction and you were to disclose the wrong fee amount, they've said that could also be problematic as well.

The good thing is that there are four enumerated exceptions from these requirements. Confidential commercial information. Again, this is some of your AI that you use to derive credit scores or other risk scores or predictors. Information that you've collected for fraud or AML type purposes. Information that's required to be kept confidential by some other law. And your MPI and supervisory information. The CFPB does note though that it's not going to apply to information that they're requesting from you that's unrelated to their account, like your internal operating procedures, financial strategies, performance marketing strategies, training programs for employees and things like that.

And so what should we do in response to this? Essentially, you might want to take actions before February 1 because this is when they said they would start enforcing this advisory opinion. For the consumer experience, what you really want to do is you want to make it easy for the consumer to request and obtain account information. Look at creating policies, procedures, and processes where you define, identify, track, and timely respond to these requests. And again, there's some pointers here on how you could define requests. The customer doesn't have to say, "I'm invoking my rights under Section 1034 to be entitled to the information." In most cases, they're probably not going to say that. That it's reasonable to require them to have to verify their identity, what you would normally do before sharing this type of information. And I listed some samples here that would be in scope of some types of requests that the consumers could make.

And the other thing that you might want to do is look at some of your fee schedules to make sure you're not charging fees to consumers for access or copies of account records. I listed some samples of fees, paper statement fees, check image or check copy fees, statement copies, account verification, account or customer research, document requests, payout quotes, QWRs, error notices. Essentially what they're saying, "We don't care how you've labeled or called the fee or categorized it on fee schedules, if you're charging the consumer access for their account information, we don't think you should be charging the fee." This isn't going to have impact on fees where you're performing services, where you're notarizing documents or doing signature guarantees, or if you're charging fees to third parties, or for example, garnishment fees.

And then the other thing that they say, if you do have a consumer who's repeatedly requesting the same information over and over again, that you can charge them if you've already previously complied by providing them that information. And with that, I'll turn it back over to Alan Kaplinsky.

Alan Kaplinsky:

Thanks to all of our speakers today. To make sure that you don't miss our future episodes, please subscribe to our show on your favorite podcast platform, Apple Podcast, Google, Spotify, or wherever you listen. And don't forget to check out our blog, consumerfinancemonitor.com for daily insights about 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 all for listening, and have a great day.