



December 29, 2023

The Honorable Rohit Chopra
Director
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Re: Required Rulemaking on Personal Financial Data Rights [Docket No. CFPB-2023-0052]

Dear Director Chopra,

On behalf of America's credit unions, we are writing in response to the Consumer Financial Protection Bureau's (CFPB or Bureau) proposed rule "Required Rulemaking on Personal Financial Data Rights" (Proposed Rule or NPRM)¹ which implements § 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).² The Credit Union National Association (CUNA) and National Association of Federally-Insured Credit Unions (NAFCU) (together, the Associations) advocate for America's credit unions and their more than 138 million members with personal and small business financial services products.

Credit unions are committed to the financial well-being of their members and their communities. This mission-driven member focus is a key reason why credit union members are among the most financially healthy in America and agree that their credit union cares about them. According to CUNA's 2022 National Voter Poll, consumers who use credit unions are 40 percent more likely than their counterparts who do not use credit unions to respond "very positively" to the fact that they "can trust" their financial institution.³ Further, credit union members are 45 percent more likely than nonmembers to respond "very positively" to the fact that their institution "cares about" their financial well-being AND are 52% more likely to say their institution "has positively impacted" their financial well-being. This sentiment reflects exactly the type of relationship

¹ See Required Rulemaking on Personal Financial Data Rights, 88 FR 74796 (October 31, 2023), *available at* <https://www.federalregister.gov/documents/2023/10/31/2023-23576/required-rulemaking-on-personal-financial-data-rights>.

² 124 Stat. 2008 (codified at 12 U.S.C. § 5533).

³ 2022 CUNA National Voter Poll.

banking that CFPB Director Rohit Chopra has stated he wanted to become commonplace in the consumer financial services markets.

We, and our member credit unions, strongly support consumers' rights to access and control their personal financial data but have a responsibility to ensure credit union members' data remains safe, secure, and private. As proposed, this rulemaking will have the unintended consequence of making credit union services less available and more expensive to those who need them the most.

The CFPB's proposal goes far beyond any reasonable interpretation of § 1033 of the Dodd-Frank Act and imposes substantial costs on credit unions in their capacity as data providers. Numerous technical requirements for API interfaces along with a directive that credit union data providers subsidize third party access to member data will result in an uneven playing field that penalizes credit unions. Unfortunately, the CFPB did not appear to consider the concerns raised about these facts by the small financial institutions during the Small Business Regulatory Enforcement Fairness Act (SBREFA) process,⁴ or those raised by the Small Business Administration's (SBA) Office of Advocacy.⁵ Instead, the CFPB appears to have had a pre-determined outcome from the outset of this rulemaking, which was further demonstrated by its refusal to extend the already short, less than 60-day comment period, which was held over multiple holidays.

The CFPB did not address cost-benefit concerns raised by a variety of stakeholders, including the SBA Office of Advocacy. For example, it stated, "As noted in the letter, the small entities that will be required to comply with the regulation are in the best position to provide the CFPB with information about the potential costs associated with the proposal, but the amount of time provided for the comments is insufficient. This information is crucial for determining the economic impact of the rule and for considering less costly alternatives as required by the Regulatory Flexibility Act (RFA)."⁶ In its letter, the SBA Office of Advocacy raised several specific areas of the proposed rule that are lacking sufficient RFA analysis. SBA Office of Advocacy further stated, "Because of the potential harm to small entities and consumers, the agency should adopt less costly alternatives."

While the Dodd-Frank Act calls upon the CFPB to promote fair and competitive markets, the plain language of § 1033 does not reflect an intention to reengineer data sharing mechanisms to alter financial sector competition. Furthermore, the commoditization of financial data driven by the CFPB's idealistic vision for open banking could result in the opposite of its intended effect:

⁴ See CUNA's Response, available at https://news.cuna.org/ext/resources/CUNA%20News/Daily/2023/-01-2023/0125231033-SBREFA-Outline-Response_280283504.pdf. NAFCU's Response, available at https://www.nafcu.org/system/files/files/1.25.23%20Letter%20to%20CFPB%20re%20Outline%20of%20Proposals%20for%20Required%20Rulemaking%20on%20Personal%20Financial%20Data%20Rights_0.pdf.

⁵ SBA Office of Advocacy Letter to CFPB, available at <https://advocacy.sba.gov/2023/12/21/advocacy-submits-comments-on-cfpbs-nprm-on-personal-financial-data-rights/> (Dec. 21, 2023).

⁶ *Id.*

rewarding the largest, most technologically sophisticated companies at the expense of credit unions and other community institutions focused on relationship banking.

Executive Summary

The Associations regard most aspects of the proposal as fatal to the development of any reasonable final rule and recommend the Bureau take additional time to conduct a more informed rulemaking process that prioritizes and incorporates the meaningful feedback provided by credit union data providers.

Notwithstanding these fatal flaws, the Associations recommend certain substantive changes to the proposed rule, the most important of which are listed below, ordered as they appear in the proposed rule (i.e., not in order of relative importance), and discussed in further detail in later comments:

1. Provide tiered exemptive relief for covered data providers;
2. Provide longer compliance timeframes with transitional relief for covered data providers;
3. Recognize a qualified industry standard before advancing a final rule;
4. Establish a framework that permits data providers to charge reasonable fees for third party access;
5. Withdraw granular technical performance specifications for the developer interface;
6. Substantially curtail the categories of covered data;
7. Exclude certain data fields in the enumerated categories of covered data to the extent the categories themselves are not substantially curtailed;
8. Issue an additional request for information to refine cost estimates before proceeding with a final rule;
9. Create a safe harbor for data providers who rely on the representations of third parties about their data security and risk management practices;
10. Establish a clear allocation of liability to third parties who mishandle covered data or abuse their consumers' trust;
11. Accommodate supervised financial institutions who offer legitimate secondary uses of covered data;
12. Establish a framework for accreditation that leverages the CFPB's supervisory resources to whitelist third parties and alleviate excessive due diligence costs for data providers; and,
13. Establish clear data security standards and an appropriate supervisory framework for third parties that access covered data.

To mitigate the harm of the proposal and the hazards of rushing to publish a final rule, the CFPB should postpone the rulemaking and engage credit unions and other data providers through industry town halls, working groups, and pilot programs, then embark upon a new, better-informed rulemaking that takes into account the many harms that smaller entities may face without a robust RFA analysis. More meaningful engagement would yield more accurate

assessments of costs, technical obstacles, and implementation timeframes, all of which the CFPB has severely underestimated.

While the Associations would prefer this approach, the CFPB has made clear that it fully intends to proceed with a radical reengineering of financial sector competition through a rushed rulemaking process.⁷ Accordingly, in the interest of mitigating substantial harm to credit unions, the Associations suggest practical alternatives to the substantive provisions of the proposed rule.

I. The Proposed Rule Does Not Comply with the Administrative Procedures Act and Exceeds the Congressional Grant of Authority for this Rulemaking

The CFPB is mandated to act within the scope of authority Congress delegated to it under the Dodd-Frank Act. In precedent first created by *Chevron, U.S.A., Inc. v. NRDC*⁸, now known as the *Chevron Doctrine*, there is a two part test for determining whether an agency interpretation of a statute is reasonable. Under the second part of the test, a court defers to agency interpretations of ambiguous statutes as long as the judge finds the interpretation to be reasonable. However, before getting to this question a court, under part one, must first determine whether the meaning of the statute addressing the precise issue before the court is clear. If the statutory text is clear, then that is the end of the matter; the court and the agency must give effect to the unambiguously expressed intent of Congress.⁹ Only when the statute is silent or unclear on the issue can a court move on to step two of the *Chevron* test. As fully discussed below, the text of § 1033 of the Dodd-Frank Act is clear.

As a general matter, CFPB rulemakings must comply with the Administrative Procedure Act (“APA”),¹⁰ which requires a reviewing court to set aside agency action under certain conditions, including when agency rulemaking is arbitrary or capricious.¹¹ When considering whether an agency may have acted in an arbitrary and capricious manner, courts generally focus on: (1) whether the rulemaking record supports the factual conclusions upon which the rule is based; (2) the rationality or reasonableness of the policy conclusions underlying the rule; and (3) the extent to which the agency has adequately articulated the basis for its conclusions.

Any rulemaking the CFPB engages in to implement a new rule or modify an existing rule faces two primary statutory requirements. First, the rule must conform to the authority set forth in the Consumer Financial Protection Act (“CFPA”). Second, there must be a “concise general statement of [the amendment’s] basis and purpose,”¹² reflecting rational and reasonable policy conclusions

⁷ See CFPB, Director Chopra’s Prepared Remarks at Money 20/20 (October 25, 2022) (“[i]ncumbents will find their customers to be less ‘sticky’”).

⁸ 467 U.S. 837 (1984).

⁹ *Id.* at 843 n.9 (*Chevron* instructs courts at step one to employ all of the traditional tools of statutory interpretation first).

¹⁰ See generally 5 U.S.C §§ 551-559.

¹¹ 5 U.S.C. § 706.

¹² 5 U.S.C. § 553.

in the rulemaking record to support the change and thus avoid being overturned as “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.”¹³

The CFPB is proposing to establish 12 CFR part 1033, to implement § 1033 of the CFPA. In 2010, Congress clearly and explicitly recognized the importance of personal financial data rights in § 1033. However, the CFPB’s NPRM goes beyond the text or intent of the statute, with minimal legislative history to support the expansive interpretation it takes of the text of the statute to require broad third-party access to consumer data that is in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, subject to certain exceptions. As outlined below in several parts of the Associations’ comments, the CFPB is ignoring the text of the Dodd-Frank Act and going beyond its Congressionally delegated authority. Additionally, its refusal to consider the feedback it received during the SBREFA process, its extremely short comment period during the Notice of Proposed Rulemaking, and incomplete analysis overlooking the disproportional cost on smaller entities, reveal a predetermined outcome. If the proposal is finalized without substantial changes to address these infirmities, it will lead to an arbitrary final rule.

II. Subpart A—General

a. § 1033.111 Coverage of Data Providers

1. Definition of Data Providers

An entity is defined as a data provider subject to the requirements of the proposal if it controls or possesses covered data concerning a covered consumer financial product or service. A covered consumer financial product or service includes a Regulation E deposit account, a Regulation Z credit card, or the activity of facilitating payments. While the scope of coverage subjects nearly all depository institutions to the proposal, it leaves out many fintech companies operating in the consumer financial service marketplace, such as payday lenders and buy-now-pay-later (BNPL) providers.

Coverage of entities that facilitate consumer payments is also unclear and the Associations request clarification as to whether this term encompasses nonbank Person to Person (P2P) providers. Also, there are other types of entities that may be involved in facilitating payments, such as third parties that allow consumers to set up bill pay arrangements. The CFPB should address what “facilitation of payments” means in the context of data provider coverage.

The Associations also request clarification of the term “wallet” in example 1 for § 1033.111(c). The CFPB is separately considering a proposed rule that would define “wallet functionality” as a product or service that “[s]tores account or payment credentials, including in encrypted or tokenized form” and “[t]ransmits, routes, or otherwise processes such stored account or payment

¹³ 5 U.S.C. § 706(2)(A).

credentials to facilitate a consumer payment transaction.”¹⁴ The CFPB should confirm whether the definition of wallet for the purpose of § 1033 will adhere to this proposed definition.

2. Gaps in Coverage

The exclusion of other fintech entities substantially involved in markets for consumer financial products and services raises fundamental questions about competitive fairness and casts doubt upon the CFPB’s primary rationale for issuing the proposal--catalyzing competition. The proposed rule favors the outflow of information from depository institutions to fintech companies due to the narrow definition of data provider. Rather than promote competition, this arrangement may in fact undermine it by driving further consolidation among credit unions and other, traditional community financial institutions, while simultaneously rewarding the largest and most technologically sophisticated entities.

Since the passage of the Dodd-Frank Act, the number of credit unions has declined by over 30 percent.¹⁵ This may be attributed to a combination of new regulatory costs, competitive pressures from larger banking entities, and more recently, operational advantages possessed by fintech companies. Implementation of § 1033 could have the effect of accelerating consolidation within the credit union industry and reducing brick and mortar financial services in underserved or rural communities.

As discussed in comments regarding the prohibition on access fees, the CFPB may wish to consider how the cost of the proposed rule to depository institutions coupled with increased competition from fintech companies may result in operational costs being passed onto consumers through indirect means. The CFPB should also consider whether readjustment of the proposed rule’s applicability to smaller credit unions is appropriate given field of membership limitations, which could significantly limit prospects for cost-recovery in an open banking environment that favors entities serving a national market.

More generally, the CFPB should conduct a more comprehensive cost-benefit analysis to understand if providing information regarding certain non-covered consumer financial products or services (such as a mortgage) truly pose fewer benefits to consumers than the more speculative benefits associated with sharing information about credit card rewards, scheduled bill payments, and product-specific terms and conditions documents.

3. Exclusions From Coverage and Recommended Relief

The proposed rule will impose significant one-time and ongoing costs on credit unions of all sizes. These costs will weigh more heavily on smaller credit unions that lack the operational sophistication to satisfy certain requirements in-house (e.g., building interfaces, responding to

¹⁴ See CFPB, Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, 88 Fed. Reg. 80197 (November 17, 2023).

¹⁵ See NAFCU, 2022 Report on Credit Unions, 20 (November 2022).

technical inquiries, evaluating the data security of third parties) and will therefore depend upon service providers. A complete dependency on service providers is likely to correspond with higher ongoing costs and reliance on largely unregulated entities to achieve compliance with the rule.

To address the harmful effects the proposed rule will have on smaller entities, the CFPB has elected to pursue a narrow exclusion for data providers that are depository institutions without any existing consumer interface. The Associations regard this exclusion as too narrow. The proposed definition of a consumer interface is broad and encompasses any interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable by consumers. Consequently, any depository institution of any size offering online banking to a consumer, even in its most limited form (i.e., viewing balances), will likely be subject to the rule. The Associations disagree with this approach.

The CFPB should instead pursue tiered exemptive relief. For data providers that offer no consumer interfaces, the existing exclusion from the rule should remain applicable. For depository institutions that meet the SBA's definition of a small business, only the requirement to provide a consumer interface should apply. For depository institutions with less than \$50 billion in total assets, minimum technical performance specifications should not apply for the developer interfaces.¹⁶

A tiered set of exemptions would better mitigate the substantial costs of the rule for institutions that lack the economies of scale or the bargaining power necessary to fund ongoing API development and maintenance. Tiered exemptions would also offset the compliance date bottleneck, described in greater detail below.

b. § 1033.121 Compliance dates

Credit unions with experience developing APIs have expressed concern that the compliance dates proposed by the CFPB are unrealistic. Additionally, the proposal will likely result in a compliance bottleneck for institutions between \$850 million and \$50 billion in total assets that must all achieve compliance within a remarkably brief span of two and a half years. There are over a thousand banks and credit unions in this cohort of institutions that will be competing for the attention of their core providers and vendors as they manage significant IT overhauls to support API development.

The proposed timeframes for implementing the rule must be readjusted. A more realistic estimate of the time needed to establish developer interfaces and complete system testing will likely be at least five years for large credit unions. However, to avoid a compliance bottleneck at

¹⁶ See Small Business Administration, *SBA Size Standards* (effective Mar. 17, 2023), https://www.sba.gov/sites/sbagov/files/2023-06/Table%20of%20Size%20Standards_Effective%20March%2017%2C%202023%20%282%29.pdf.

any given point in time, the CFPB should further divide each cohort of institutions to space out compliance deadlines over a longer period.

The Associations recommend dividing each of the last two cohorts of data providers (i.e., institutions with less than \$850 million in total assets and institutions between \$850 million and \$50 billion in total assets) into additional groups with a one-year interval between them for the purpose of determining compliance deadlines. A total of four groups would be appropriate for segmenting the two existing cohorts that account for institutions under \$50 billion in total assets. Additional segmentation and an extension of compliance deadlines would not prevent data providers from voluntarily complying by an earlier date but are critical to the successful implementation of the open banking framework by small data providers.

If the CFPB does not pursue the alternative exemption standards discussed in the previous section, it should also consider a compliance phase-in for smaller institutions. As proposed, the existing exclusion from data provider coverage is more harmful than helpful to very small institutions that may purposefully avoid development of digital banking services to avoid new compliance costs. A decision not to offer digital banking, even in basic form, could threaten competitive viability in today's crowded financial services market.

Small financial institutions must have the ability to participate in the open banking ecosystem without being priced out of it. An appropriate phase-in for small institutions should postpone compliance for developer interface requirements until at least four years after their initial compliance date (i.e., establishing a compliant consumer interface). If the CFPB has a genuine desire to promote competition rather than consolidation, then it should consider such relief as the bare minimum.

Lastly, the CFPB should clarify how it will assess compliance with the interface-related provisions of the proposed rule, particularly during an initial period of implementation. Will a data provider be required to demonstrate fully functional interfaces, onboard all interested third parties, and disable all screen scraping of covered data following the effective date? As noted in later comments, onboarding third parties will take time and a total cutoff of existing data access arrangements may frustrate consumers. The CFPB should tailor its compliance expectations for data providers to account for transitional uncertainty and provide ample runway for operational testing as third parties request interface access.

c. § 1033.131 Definitions

In general, the Associations regard the substance of the proposal rather than its underlying definitions as problematic. However, certain defined terms would benefit from clarification.

The proposed definition of consumer interface should be clarified so credit unions can better ascertain whether they are covered data providers. As noted previously, the proposed definition of a consumer interface is broad. The CFPB should explain whether a consumer accessing a web

page or secure inbox to view a PDF of a transaction statement is equivalent to a data provider receiving a request for covered data and making it available in electronic form.

The CFPB should also clarify elements of the data aggregator definition. For example, what does “retained by” mean in the context of a third party that uses a wholly-owned subsidiary as an aggregator for accessing covered data? What is meant by the phrase “enable access to covered data” in the context of a credentialing service that facilitates a data provider’s risk management and data security review? Does the “enabling access” prong of the definition require a data aggregator to be the party actually connected to a developer interface?

Additionally, the proposed rule’s prohibition on secondary uses of data requires the CFPB to clarify the terms “targeted advertising” and “cross selling.” Further clarification on the meaning of “reasonably necessary” in the context of **§ 1033.421** is also crucial.

The Associations ask that the CFPB clarify certain elements in the definition of a qualified industry standard, as discussed below.

d. § 1033.141 Standard setting

The CFPB’s vision for open banking largely depends on private industry embracing standards for data exchange that meet the definition of a qualified industry standard. The CFPB has wisely chosen not to promulgate its own technical specifications, but still retains ultimate authority as far as recognizing future standards. The CFPB has not recognized a qualified industry standard or outlined any plan for when it intends to do so. The lack of clarity around timing has created uncertainty for the entire credit union industry. The longer this uncertainty persists, the more difficult and costly it will be to implement a final rule.

The Associations urge the CFPB to identify at least one qualified industry standard before advancing any final rule. Additionally, to ensure that data providers and their vendors are adequately prepared to meet the requirements of a recognized standard, the CFPB should provide at least one year of runway between the designation of a qualified industry standard and publication of a final rule.

Deferring publication of a final rule until after a qualified industry standard is recognized will grant the CFPB time to refine assumptions about costs, feasibility, and deadlines based on the technical requirements associated with the standard. Furthermore, a modest delay between recognition of a qualified standard and a final rule will allow the CFPB to perform a more realistic assessment of vendor readiness.

Some credit unions and banks have already begun to align API development around at least one data exchange standard.¹⁷ The CFPB should acknowledge this existing alignment when it does

¹⁷ See FDX, Member Registry, available at <https://registry.financialdataexchange.org/>. As of December 2023, twelve credit unions are members of FDX.

recognize a qualified industry standard. While recognition of multiple qualified industry standards is desirable in the long run, provided they are interoperable and freely available, the CFPB should aim to reduce industry uncertainty as soon as possible by recognizing a standard that already has significant industry support.¹⁸

Failure to recognize a standard that possesses indicia of industry adoption today would have profound consequences for credit unions and other institutions that have already made significant investments to align API development around a particular specification. If the CFPB were to ignore existing industry support for such a standard or fail to recognize one before publication of a final rule, widespread uncertainty would greatly complicate implementation of a future rule.

1. Definition of Qualified Industry Standard

The Associations also request clarification of the term “qualified industry standard.” As defined in the proposal, a qualified industry standard is one issued by a standard-setting body that is fair, open, and inclusive in accordance with § 1033.141(a).

In general, a standard setting body is fair, open, and inclusive when it has the following attributes:

1. Openness: The sources, procedures, and processes used are open to all interested parties.
2. Balance: The decision-making power is balanced across all interested parties, including consumer and other public interest groups, at all levels of the standard-setting body.
3. Due process: The standard-setting body uses documented and publicly available policies and procedures, and it provides adequate notice of meetings and standards development, sufficient time to review drafts and prepare views and objections, access to views and objections of other participants, and a fair and impartial process for resolving conflicting views.
4. Appeals: An appeals process is available for the impartial handling of appeals.
5. Consensus: Standards development proceeds by consensus, which is defined as general agreement, but not unanimity.
6. Transparency: Procedures or processes for participating in standards development and for developing standards are transparent to participants and publicly available.
7. CFPB recognition: The standard-setting body has been recognized by the CFPB within the last three years as an issuer of qualified industry standards.¹⁹

With respect to the balance component, the CFPB should clarify what is intended by the statement that “[n]o single interest or set of interests dominates decision-making.”²⁰ The CFPB

¹⁸ For example, FDX has developed a specification that is actively used by several credit unions and supports dozens of in-market API connections.

¹⁹ 88 Fed. Reg. 74807.

²⁰ *Id.*

might address whether a dominant interest is one that disproportionately benefits a specific type of commercial entity, or organizations of a certain size. Further discussion of this aspect of balance would offer needed context for the parallel requirement to achieve “meaningful representation for large and small commercial entities.”

In the event the CFPB fails to recognize a qualified industry standard before publication of a final rule, the agency should adopt an additional, presumptive category of qualified industry standard. This category should recognize that a commercially reasonable standard for the purposes of §§ 1033.311(b)(2), (c)(1)(ii), 1033.321(b), 1033.331(e), 1033.351(b)(1) and (c)(3) becomes a qualified industry standard if it is used by more than one data provider for a period of at least one year after beginning compliance with a final rule. Once a qualified industry standard is identified, a credit union should have a grace period for transitioning away from any interim standard to the qualified standard.

The purpose of a presumptive category would be to assure entities that have adopted any interim standard in the absence of a qualified industry standard that the CFPB’s expectations will not change from year-to-year regarding what is commercially reasonable. It would be unfair to credit unions and other data providers to demand frequent reconfiguration of APIs to satisfy an amorphous standard of reasonableness—particularly in an environment where the CFPB is unable to offer certainty through standard recognition.

The CFPB should also clarify how the seventh element in the list (CFPB recognition) would operate on an ongoing basis. Will a standard setting body need to periodically petition the CFPB for recognition after each three-year period? If the CFPB chooses not to recognize a previously established qualified industry standard, how will it examine entities that are substantially reliant on that standard? To mitigate potential confusion and future uncertainty, the Associations ask the CFPB revise the seventh element by striking the reference to “within the last three years.”

Conditioning the future availability of a qualified industry standard on periodic CFPB reapproval subjects data providers to unnecessary doubt. Furthermore, it is unlikely the CFPB will be able to unwind industry reliance on a qualified industry standard even if it decides to withhold recognition in the future. The financial sector’s experience decommissioning the LIBOR should serve as a reminder that an industry-wide decoupling from a prevalent standard or benchmark would be, at best, an expensive, multi-year endeavor.

III. Subpart B—Obligation to Make Covered Data Available

a. § 1033.211. Covered Data

Dodd Frank § 1033(a) provides:

“Subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person

concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges, and usage data. The information shall be made available in an electronic form usable by consumers.”

The categories of information the Bureau envisions would be required to be made available by covered data providers goes beyond the scope of the statute and must be significantly pared back. This is another example of the CFPB’s overreach. The categories of information outlined for covered data providers in the proposed rule clearly exceed the statutory intent. This is not permissible. § 1033(a) of the Dodd-Frank Act is not ambiguous.

The Bureau directs in the preamble to the proposed rule that “[t]hese examples are illustrative and are not an exhaustive list of data that a data provider would be required to make available under the proposed rule.”²¹ The final rule should clearly and explicitly provide exactly what data points data providers are required to share to remove any uncertainty surrounding the data provider’s obligations. The Bureau also seeks comment on the benefits and data needs for consumers who are in the process of switching accounts. That request begs the question, what prompts a member to recognize the benefits of switching accounts? In the absence of cross-selling or targeted advertising, there will be no prompts highlighting these benefits. The proposed rule arguably does not allow a third party to let a consumer know of the benefit(s) of switching accounts because it does not permit secondary uses.

1. Transaction Information

It is clear from the legislative text that information regarding settled transactions and deposits should be made available under the final rule. To ease compliance and limit the burden on data providers, the Bureau should include a clear list of those elements contained within this category that is consistent with existing regulatory requirements including Regulation Z, Regulation E, and Regulation DD.

Requiring the inclusion of pending transaction information could be problematic because these transactions are continually subject to change until the transaction settles. Given the “snapshot in time” nature of the data requests under this proposed rule, the pending transaction information could be outdated immediately following the data request causing, at a minimum, consumer confusion, and potentially serious consumer harm if outdated information is used to make decisions about products and services offered to the consumer. For this reason, the Bureau’s intended beneficial consumer use cases of “fraud detection and personal financial management” are not supported by the inclusion of pending transaction information. Attempts by third parties to maintain the most current pending transaction data by continually making

²¹ See NPRM at 56.

requests through the interface would quickly overwhelm data providers' systems and increase the cost for data providers.

Information regarding rewards credits should not be included as a required data element. Rewards are frequently managed separately from the financial institution's core banking platform and there is currently no consistency in how rewards are handled. Requiring the inclusion of this data element will create an undue burden for financial institutions that will not provide consumers with a commensurate benefit.

The CFPB should limit the amount of historical transaction data that data providers must make available to 12 months. Some credit unions may not store historical information about a consumer account in the same systems that generate current statements for members. Accessing historical information may correspond with greater time and effort for credit unions and it may be the case that certain data elements will be reported differently for different time periods depending on the use of particular systems, formatting, or vendor solutions. For older information not kept in a standardized format, or current data susceptible to variances in formatting (e.g., records related to automatic bill pay), the CFPB should recognize that such information cannot be efficiently retrieved in the ordinary course of business.

2. Account Balance

The inclusion of account balance as a data element required to be shared under this rulemaking is appropriate. We do not object to the inclusion of this information; however, the CFPB should also explicitly include remaining credit availability as a data element of this category.

3. Information to Initiate Payment to or from a Regulation E Account

The Associations agree that the transmission of routing and account numbers outside of secure payment systems could expose credit unions to a significant risk of fraud if the information is lost or mishandled by a third party. Credit union members would also face corresponding privacy risks and potentially greater exposure to identity theft.

While tokenized account and routing numbers (TANs) are industry innovations that help mitigate fraud risk for both consumers and financial institutions, they are relatively new advancements that many small financial institutions have not yet adopted. TANs can be costly, and implementation is dependent upon the financial institution's service partner and their offerings. For this reason, many of the most vulnerable data providers would not be able to take advantage of this innovation and protection from the start causing significant market inequities that could exacerbate the impact of bad actors taking advantage of a new system.

Therefore, the final rule should exclude this category of covered data to protect financial institutions and consumers until a time at which tokenized account and routing numbers have reached ubiquity in the marketplace.

4. Terms and Conditions

The final rule should not include terms and conditions as a category of covered data in this rulemaking. The stated beneficial use cases for this data, “comparison shopping and personal financial management,” are not supported by the rule in its current form given the prohibition on secondary uses of data, including cross-selling. Moreover, the cost and burden for data providers to manage product-level terms and conditions documents and to make those conveyable through data fields in an API would vastly exceed the benefit to consumers.

Additionally, there is no well-established use case for this information. In discussions with aggregators, they reported a lack of demand for terms and conditions documents, and they also stated that they are not currently equipped to handle this data if they did receive it. This data element is also not required or scoped by issuers of industry standards, such as FDX. Mandating financial institutions provide this information exceeds the Bureau’s statutory authority under § 1033.

The proposed rule’s requirement that data providers share with third parties information about whether a consumer has entered into an arbitration agreement is beyond the scope of covered data in this rulemaking and will only make consumers targets for predatory attorneys mining for litigation opportunities. Arbitration reduces transaction costs and enables fair, speedy, and efficient dispute resolution, thereby providing significant advantages to consumers. The inclusion of this data element contradicts the CFPB’s assurances in a separate rulemaking regarding covered form contracts used by nonbanks. In that rulemaking the CFPB stated that it had no intention of collecting legal terms and conditions from depository institutions.

5. Upcoming Bill Information

The value of this category of information is unclear given the general operational procedures for scheduled bill payments: both one-time and recurring. The proposed rule envisions a consumer scheduling these payments with their financial institution for extraction to the payee when in reality, the consumer almost always schedules these transactions through the payee’s platform. Furthermore, even if a consumer arranges their bill pay through the data provider, the provider will often be unaware of the amount due in advance.

Recipient data used in automatic bill pay systems may not reside within a single repository or have standardized formatting. Automatic billing systems may also have idiosyncratic features that are contingent upon a credit union’s core provider, vendor solution, or the payment channel selected by the member or credit union to transmit payment. To the extent that cores can be leveraged to help make this data available, smaller credit unions will be challenged to make such data available if their core is not providing all elements of this service to consumers. This could stifle competition by providing an edge to core providers who know that financial institutions not using their services for all elements of covered data may find it difficult to make all categories

available via the API-based interfaces. Collectively, these differences would make it challenging for a credit union to consolidate and export in a standard format information from bill pay systems—particularly if rules for payment scheduling are governed by proprietary business logic dictated by vendors.

It is also unclear whether the scope of covered accounts is even sufficient to yield meaningful visibility about automatic payments. Recurring debit transactions arranged through a merchant are distinct from recurring bill pay arranged through a credit union. Recurring payments initiated by merchants as part of a subscription service may not even register as “automatic” or “recurring” when presented on an account statement, and some studies have shown that consumers may not realize that they are even enrolled in auto pay with a merchant.²² Accordingly, given the limited scoping of the proposals under consideration, data providers would need to undertake significant technical overhauls to consolidate and standardize bill pay data that may not even reflect the majority of a consumer’s recurring charges.

Further, the Bureau’s use case of personal financial management is already addressed by providing historical transaction information, making the inclusion of this category duplicative. As for consumers who are switching accounts, data does not equal the transaction. Standing authorizations do not transfer between organizations and the consumer must once again set up the scheduled payment with the new provider under network rules.

Due to this information residing in multiple systems, upcoming bill information cannot be provided in the ordinary course of business and should be excluded from the definition of covered data. If the Bureau chooses to move forward with the inclusion of this category, it should be limited to those upcoming bill payments that are specifically originated with the data provider.

6. Basic Account Verification Information

The CFPB proposes that account identity information is necessary for account verification in the authorization process. This use case would be unnecessary if the Bureau were to shift the responsibility for obtaining consumer consent to access the information to the data provider. Further, authentication of the consumer must be performed by the data provider before responding to a request for information by a third party.

The veracity of account verification information with data providers must also be considered. Accounts, especially those established for many years, may have multiple addresses, phone numbers, or email addresses associated with them. Financial institutions tend to retain multiples of these data points over time. Data providers must not be held liable for errors or inaccuracies in the information.

²² See Nicole Specter, “35 Percent of Americans Are Enrolled in Auto Pay – and It’s News to Them,” NBC News (Aug 29, 2017), *available at* <https://www.nbcnews.com/business/consumer/35-percent-americans-areenrolled-auto-pay-it-s-news-n797131>.

b. § 1033.221. Exceptions to Covered Data

Dodd Frank § 1033(b) also sets forth four exceptions to the requirement to provide data to a consumer:

1. Any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors;
2. Any information collected by the data provider for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;
3. Any information required to be kept confidential by any other provision of law; and
4. Any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information.

We are concerned about the cost of market failures in this proposed marketplace that requires credit unions to give free access to its financial data or other proprietary intellectual property. The free rider problem is an issue in economics. That is, it is an inefficient distribution of goods or services that occurs when some individuals are allowed to consume more of a shared resource or pay less than their share of the costs. Without a careful allocation of costs of innovation, monitoring, and control of data, the incentive to create and allow access to data will reduce.

To counteract the free-rider problem and to protect consumers, these exceptions must be interpreted with a broad stroke. The Bureau's analysis of these exceptions displays an intent to adopt the narrowest interpretation. This approach harms consumers and runs counter to the spirit of § 1033, the Dodd-Frank Act, and the mission the Bureau itself. Allowing wide swaths of private consumer financial information to be shared with third parties without proper guiderails invites fraud and consumer harm.

This broad approach to the exceptions must allow credit unions to exercise reasonable judgement to prevent sharing confidential information that might cause competitive harm, endanger consumers, or undermine activities aimed at combatting fraud. § 1033 of the Dodd-Frank Act clearly and explicitly outlines exceptions to requirements in providing information to consumers. Here, again, the CFPB is ignoring the directives from Congress and making arbitrary determinations.

1. Confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors.

The Associations have concerns with the CFPB's decision to interpret the phrase "confidential commercial information" so narrowly as to only consider its meaning within the context of §

1033.²³ The CFPB should adopt a more refined interpretation of confidential commercial information that draws a distinction between data that might be useful for a consumer for consumer purposes versus data that would be of primarily commercial value (such as metadata regarding the exact time and place of transactions). Credit unions should not be required to reveal analytically enriched data if the consumer does not ordinarily see such data and cannot be said to substantially rely upon it when making decisions about the selection of consumer products or services.

The final rule's interpretation of this exception must make clear that it also includes information that cannot be shared for contractual reasons such as data transformations that occur outside the core platform like smoothing the name of a merchant in online banking portals. Confidential commercial information must also extend to attorney work product related to an account and any active litigation.

2. Information collected for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct.

As discussed below, we regard information related to transaction risk scoring as exempt information since it primarily serves to detect and prevent fraud. Additionally, information related to security incidents, such as activity logs, geolocation information, or other behavioral metadata, should also be categorized as exempt since it serves to prevent unlawful access to a consumer's account. Internal account notes and flags about activity should also be included under this exclusion. A credit union would not typically share this information outside its own organization unless interacting with a trusted third party such as a cybersecurity vendor. The CFPB should also recognize that some information collected for the purpose of preventing fraud may also be used for other analytical purposes.

The CFPB states that certain data elements, such as the location of a transaction, would not be considered exempt, but fails to explain how such data—which is actually used to prevent and detect fraud—is beyond the scope of the exemption. We recommend the Bureau reconsider this position and provide greater clarity with respect to data elements that may have both antifraud and commercial value.

3. Information required to be kept confidential by any other provision of law.

The Associations do not object to the interpretation of this exception but suggest that the Bureau enumerate, in a future small entity compliance guide, example of laws (both federal and state) that would require a data provider to withhold information from a consumer attempting to exercise § 1033 rights. The CFPB should also adopt a good faith compliance standard for data providers that withhold information if they reasonably believe it is required to be kept confidential by law. This exception category should include the Freedom of Information Act (FOIA)

²³ See NPRM at 64.

and is even referenced in a related section of the Dodd-Frank Act—§ 1034(c)—relating to a covered institution’s obligation to respond to consumer requests for information.²⁴ Courts have interpreted FOIA exemption 4, which protects trade secrets as well as commercial and financial information, to include records that “relate to the income-producing aspects of a business.”²⁵

4. Information that the covered person cannot retrieve in the ordinary course of its business.

The proposed rule offers no clarity with respect to how this exception will be interpreted. Somewhat related to this exception is the proposed rule’s attempt to define current and historical information that data providers would be required to make available to consumers or authorized third parties.

Some credit unions may not store historical information about a consumer account in the same systems that generate current statements for members. Accessing historical information may correspond with greater time and effort for credit unions and it may be the case that certain data elements will be reported differently for different time periods depending on the use of particular systems, formatting, or vendor solutions. For older information not kept in a standardized format, or current data susceptible to variances in formatting (e.g., records related to automatic bill pay), the CFPB should recognize that such information cannot be efficiently retrieved in the ordinary course of business.

As a more general matter, the CFPB should also be cautious about defining a broad range of information that a data provider must make available to a consumer. An expansive interpretation of information categories subject to § 1033 rights could incentivize data providers to collect less information about their consumers to minimize implementation costs or the risk of competitive harm. This behavioral shift in response to a burdensome future rulemaking would ultimately disadvantage consumers by depriving primary account holding institutions, such as credit unions, of critical analytical insights. Accordingly, we recommend the Bureau adopt a standard whereby data providers may exercise reasonable business judgment to determine whether information can be retrieved in the ordinary course of business rather than enumerate many specific data elements that all institutions will have an obligation to provide.

IV. Subpart C—Establishing and Maintaining Access

In general, the Associations regard the CFPB’s interpretation of § 1033 as overbroad and not in line with the intent of Congress. The legislative history of § 1033 does not support a conclusion that the CFPB was delegated authority to address major questions such as whether financial institutions can be compelled to develop APIs to support “open banking” free of charge and in accordance with granular performance specifications.

²⁴ 12 U.S.C. § 5534(c).

²⁵ See *Pub. Citizen Health Research Grp. v. FDA*, 704 F.2d 1280, 1290 (D.C. Cir. 1983).

The proposal's myriad other requirements, such as those related to developer interfaces, go far beyond the plain language of the statute and are mainly borne by data providers in order to achieve the CFPB's arbitrary vision for open banking—a vision that is seemingly inspired by the laws of foreign jurisdictions.²⁶

a. § 1033.301 General requirements

1. Requirement to establish and maintain interfaces.

The proposal requires covered data providers to maintain a consumer interface and establish and maintain a developer interface. While the CFPB's decision to orient its data sharing framework around APIs is commendable from a security perspective and reflects the technological direction well-resourced credit unions are already working towards, a mandate for data providers to develop APIs will involve substantial costs and ignores numerous practical challenges.

Data providers' existing contractual relationships with many different systems that store covered data will require significant customization of APIs and will likely involve the participation of multiple vendors.²⁷ Credit unions have reported that contracts with vendors to customize APIs for specific reporting purposes often correspond with substantial fees. These fees, when multiplied across multiple vendors responsible for different data systems (credit card rewards, bill pay, etc.) will result in significant one-time and ongoing costs for credit unions of all sizes.

2. Underestimation of Costs

As an initial matter, the estimation of costs under this proposal is challenging for all data providers due to the novel regulatory requirements involved and uncertainty surrounding the actual scope and complexity of API development necessary to support compliant interfaces. Notwithstanding those difficulties, the CFPB significantly underestimates the cost of developing and maintaining interfaces by adopting an unreasonable range of per account costs.

The CFPB asserts that the relevant metric for estimating costs for a compliant developer interface is cost per account "for data providers *generally*."²⁸ The CFPB then claims that the "reported cost of an in-house developer interface per customer or account ranges from \$0.25 to \$8 per year, with a median of \$3.37 per year." Presumably these figures are generated by taking the estimated, in-house development costs provided by larger institutions in the Provider Collection and dividing them by total number of accounts at those institutions. The result is a per-account cost derived

²⁶ See 88 Fed. Reg. 74817; see also Basel Committee on Banking Supervision, Report on open banking and application programming interfaces, 5 (November 2019), available at <https://www.bis.org/bcbs/publ/d486.pdf>.

²⁷ See CFPB, Final Report of the Small Business Review Panel on the CFPB's Proposals Under Consideration for the Required Rulemaking on Personal Financial Data Rights, 38 (March 2023) [hereinafter SBREFA Final Report].

²⁸ 88 Fed. Reg. 74848 (emphasis added). Despite per-account costs being derived from information offered by large data providers estimating their in-house development costs, the CFPB applies per-account costs to all data providers.

from a limited sample of large institutions that does not represent the market as a whole—a fact the CFPB admits in the proposal.²⁹

Not only is the CFPB’s approach flawed based on the limited sample size of larger institutions, the actual cost estimates, when applied to smaller institutions, yield a remarkably inaccurate picture of what ongoing costs would look like in an in-house development scenario.

The NCUA’s September 2023 Call Report data shows that the number of credit unions between \$100 million and \$500 million is 1,058. Collectively these credit unions have 17.3 million members. On average, a small credit union in this asset range might have somewhere between 14,000-16,000 members.

Using the CFPB’s own estimates for the ongoing cost of establishing and maintaining a compliant developer interface in-house (\$8 per account/year to reflect smaller institution economies of scale), a 14,000-member credit union would incur an annual ongoing cost as low as \$112,000 per year (assuming one member corresponds with one account)—a severe underestimate.

To illustrate how far this misses the mark, the estimated cost would be significantly less than the ongoing cost of offering a noncompliant (and far less complex) online financial account portal through a core provider—which ranges from \$200,000 to \$280,000 per year based on estimates provided by small entity representatives (SER) in the CFPB’s SBREFA Final Report.³⁰ It would also be less than the estimated cost of establishing and maintaining the multiple APIs necessary for a compliant interface.³¹

The CFPB’s analysis implies that smaller credit unions might be better off developing their interfaces entirely in-house, since it would be apparently cheaper on an ongoing basis than using a core provider. Of course, this does not reflect market reality.³² The Associations request the

²⁹ See 88 Fed. Reg. FN 164 (“[T]he data from these collections are **likely not representative of the market as a whole**. The data are informative about the practices of **some large data providers** and a selection of data aggregators and similar third parties”) (emphasis added); see also 88 Fed. Reg. 74802 ([T]he CFPB issued two sets of [...] market monitoring orders to collect information [...] one set of orders was sent to a group of data aggregators (Aggregator Collection); the second to a **group of large data providers** (Provider Collection). The information gathered through these orders informs this proposed rule.”) (emphasis added).

³⁰ See SBREFA Final Report at 37.

³¹ In the SBREFA Final Report, some SERs noted that building a compliant portal in-house would require building multiple internal APIs (3-8). One SER noted that the estimated that each of these APIs could cost approximately \$60,000 in staffing costs and \$20,000 in technology costs. See SBREFA Final Report at 37. The CFPB characterized these costs as “upfront” but a submission by that SER included in the report’s appendix offers different context: “These expenses do not include necessary maintenance and care needed after the API is deployed into a production environment. The approximate costs in personnel hours are \$60,000, with another \$20,000 for hosting the API.” SBREFA Final Report at 52.

³² See *id.* at 36-38 (“Overall, SERs expressed that the CFPB’s cost estimates for depository data providers were too low.”). Elsewhere in the SBREFA Final Report, the CFPB states that “[s]everal SERs noted that depository data providers would likely have to rely on core service providers to help provide a portal.” *Id.* At 37.

CFPB gather additional data regarding costs through a separate RFI that covers a more representative sample of institutions before proceeding with a final rule.

Notwithstanding the unusual result of applying the CFPB's estimates to smaller institutions, the CFPB's mid-range estimate of \$5 per account per year results in extraordinarily *high* costs for moderately sized credit unions developing APIs in house. The CFPB's analysis of larger data providers' responses to the Provider Collection reveals a median estimated cost of \$21 million *per year* for establishing and maintaining a developer interface.³³ Notably, this estimate reflects the economies of scale available at larger data providers sampled in the Provider Collection.

Based on the NCUA's September 2023 Call Report data, there are 424 credit unions with assets greater than \$1 billion. Collectively, these credit unions serve 100 million members. On average, a credit union in this asset range serves approximately 236,000 members and would incur an annual cost of \$1.18 million if it is deemed a "medium-sized depository" (again, assuming one account per member). Furthermore, using the CFPB's \$5 per account per year estimate as a baseline for total, ongoing industry costs, the market-level impact of the proposal would be greater than any other CFPB rule derived from the Dodd-Frank Act.³⁴

Another significant flaw in the CFPB's analysis of costs is the agency's assumptions about ongoing costs for smaller institutions using a core provider to achieve compliance with the rule. In the proposal, the CFPB claims that fees charged by core banking providers to develop interfaces can "be up to \$24 per account per year" and cites to a portion of the Final SBREFA Report which states the following:

"SERs stated that core service providers are likely to charge data providers a per-account, per-month fee for use of the portal. SERs noted this was similar to pricing for providing online financial account management portals. **One data provider** SER expressed that these costs could be as high as \$2 per account per month."³⁵ (emphasis added)

Notwithstanding the fact that \$24 per account per year likely underestimates the total ongoing cost of contracted API services, the CFPB cannot pin the bulk of its analysis on one SER's estimate. The Associations request the CFPB postpone the rulemaking to conduct additional market research. The Associations also recommend the CFPB use such an opportunity to collect more thorough, accurate, and inclusive information regarding the costs incurred by entities with

³³ It is unclear from the CFPB's analysis whether the cost of "establishing and maintaining" interfaces is derived from annualized up-front and ongoing costs.

³⁴ For comparison, the CFPB's estimated total *market-level impact* of the HMDA Rule on ongoing compliance costs was approximately \$67,300,000 in 2018. See CFPB, Report on the Home Mortgage Disclosure Act Rule Voluntary Review, 7 (March 2023).

³⁵ See SBREFA Final Report at 38.

partially compliant interfaces. As the CFPB itself acknowledges, limited data in this area also hinders analysis.³⁶

Even assuming that the CFPB's estimate is reasonable, \$24 per account per year would still translate into enormous costs for credit unions that are deemed small according to the SBA's size standards. For example, a credit union in Kansas with around \$750 million in total assets serves more than 60,000 members. Despite being small, the credit union, would spend \$1.4 million per year to achieve compliance based on the CFPB's \$24 per account per year estimate. This ongoing cost would be roughly a quarter of the credit union's year-to-date net income, as reported on September 2023.

Significant differences between the proposal under consideration included in the SBREFA Outline and the current proposal also warrant careful reexamination of estimated costs.³⁷ A common complaint from credit union SERs during the SBREFA process was a lack of concrete detail in the proposals around specific cost-plus features of the rule. Absent clearly defined requirements in the Outline, cost estimates varied widely and did not take into account certain key aspects of the current proposal (e.g., the prohibition on access fees).

The impact of the implementation costs for this proposal is especially potent for credit unions. As not-for-profit, member-owned cooperatives, credit unions do not have the same opportunities to raise capital as other data provider peers. The timing of this proposal is also problematic for credit unions' bottom line because this proposal cannot be viewed in a vacuum. Credit unions' non-interest income is currently under attack from all angles including the Federal Reserve Board's proposed reduction in debit interchange fee revenue and the CFPB's own pressure on fees including overdraft, NSF, and credit card late fees. The structure of credit unions means that any costs associated with this proposed rule's requirements will accrue directly to the member-owners, i.e., consumers. Any new requirements under § 1033 should consider the impact on financial institutions with respect to size and sophistication as well as the ability to fulfil their member needs. Like many mandated aspects of banking operations, there are significant fixed costs involved in enabling third party data access. These fixed costs impose a disproportionate burden on smaller institutions—a group that includes most credit unions—with less scale across which to amortize these costs.

The CFPB cannot reasonably fulfill its obligations under the SBREFA to estimate the impact on small entities by issuing a proposal that diverges significantly from what was presented in the

³⁶ See 88 Fed. Reg. 74848 (“[T]he CFPB cannot provide a precise estimate of the cost of bringing such systems into compliance with the proposed rule. However, that cost would generally be a fraction of the cost of developing and maintaining a new interface, as described above.”).

³⁷ See 88 Fed. Reg. 74814 (“[T]he CFPB notes that the proposed rule differs in many respects from the CFPB's proposals under consideration.”).

Outline.³⁸ Furthermore, comparison of large institution costs (i.e., the Provider Collection) with best estimates given by SERs in response to a nonrepresentative set of approaches discussed in the Outline cannot provide a reasonable picture of costs under the current proposal.

3. Prohibition on Fees

The proposal would prohibit a data provider from charging any fee or charge to a consumer or third party in connection with accessing an interface or receiving requests to make covered data available. The Associations regard this prohibition as unreasonable and unlikely to achieve its intended effect.

Credit unions and other data providers will need to recoup the substantial costs associated with establishing and maintaining compliant interfaces. Some institutions may have no choice but to pass these costs onto consumers in the form of higher account maintenance fees.³⁹ While larger institutions may be able to subsidize interface development to avoid charging additional fees, variations in account pricing between large and small institutions would likely exacerbate competitive differences. These differences would be especially acute for credit unions as discussed above. These differences would not “catalyze” competition in the way the CFPB intends, but rather accelerate industry consolidation by rewarding the largest incumbents.⁴⁰

While it may be reasonable to limit fees for access to consumer interfaces, a prohibition on charging third parties for the privilege of accessing an API paid for by the data provider is misguided. For data providers that are reliant on service providers to achieve compliance with the rule, the proposal leaves no meaningful mechanism to manage and negotiate costs. As the Director has noted, “In a market where small financial institutions need to compete head-to-head with big players, I am concerned that the core services providers that small players rely on have too much power in the system.”⁴¹

If the CFPB intends to prescribe granular requirements for API development while simultaneously placing the duty of risk management entirely on data providers, it must explore mechanisms for balancing the uneven distribution of burden created by the proposal. The best way to achieve a fairer rule would be to postpone the rulemaking and invite additional more specific consideration of the concerns SERs have raised previously but which the CFPB has decided to ignore. The CFPB

³⁸ See Regulatory Flexibility Act, 5 U.S.C. § 609(5) (stating SERs shall consider the findings under 603(b)); see also 5 U.S.C. § 603(b) (the initial RFA analysis shall include “a description of the projected reporting, recordkeeping and other *compliance requirements* of the proposed rule.”) (emphasis added).

³⁹ See SBREFA Final Report at 29.

⁴⁰ See SBREFA Final Report at 54, Comment of Union Square Credit Union.

⁴¹ CFPB, Director Chopra's Opening Remarks to the Community Bank and Credit Union Advisory Councils (April 7, 2022), available at <https://www.consumerfinance.gov/about-us/newsroom/director-chopras-opening-remarks-to-the-community-bank-and-credit-union-advisory-councils/>.

should also permit data providers to charge reasonable fees for third party access instead of adopting a bright line prohibition.

b. § 1033.311 Requirements applicable to developer interface

1. Standardized Format

The proposal requires a developer interface to make available covered data in a standardized format. A developer interface is compliant in this respect if it adopts a data format set forth in a qualified industry standard, or in the absence of a qualified industry standard, makes available covered data in a format that is widely used by the developer interfaces of other similarly situated data.

The CFPB should clarify that the mere existence of a qualified industry standard will not serve to disqualify any alternative but reasonable approaches used by data providers. Although the Associations encourage the CFPB to identify a qualified industry standard as soon as possible, and preferably one that already possesses indicia of industry alignment, the CFPB should accommodate alternatives. If a data provider chooses an alternative data format, the recognition of a qualified industry standard should not disqualify reasonable alternatives, which could later mature into additional qualified industry standards.

As currently proposed, the “widely used” prong of the alternative standard would be heavily influenced by phased implementation going from largest to smallest institutions. This could have the effect of favoring a standard used by larger institutions which could result in competitive disparity—especially in matters related to technical performance specifications. Accordingly, the availability of § 1033.311(b)(2) should persist even after recognition of a qualified industry standard.

In an environment where multiple qualified industry standards exist, or other reasonable alternatives are widely adopted, the CFPB should clarify that neither a consumer nor a third party has any right to compel a data provider to adopt any particular standard. This arrangement would promote healthy competition and ensure that standard setting is not disproportionately influenced by the largest institutions.⁴²

2. Performance specifications

The proposed rule would require developer interfaces to satisfy minimum performance specifications and adhere to minimum downtime specifications. The Associations regard these

⁴² For example, a qualified industry standard might favor larger incumbents by setting forth a near-zero minimum downtime requirement, which would favor companies with the greatest resources while achieving only marginal benefits for consumers.

requirements as overly burdensome and not in line with the Department of the Treasury's directive that "[w]herever possible, regulation should be tech neutral."⁴³

The CFPB has proposed that a proper response rate for a developer interface is one that sends a response within 3,500 milliseconds. The CFPB does not reference any particular source as the basis for setting a 3,500-millisecond benchmark. The Associations regard this proposed response time as arbitrary and out of line with the realistic performance characteristics of a system pulling different quantities of information from multiple APIs. For example, members of the Associations have expressed doubt that a response can be given in such a short timeframe if a third party requests the entire historical period for a member's covered data.

The format of the data may also influence response time. Without recognition of a qualified industry standard, it is impossible to predict the overall performance characteristics of an API transmitting different types of covered data. Accordingly, the Associations request the CFPB withdraw this requirement.

The Associations also object to a minimum downtime requirement that is defined loosely as anything the CFPB deems reasonable. The CFPB should clarify that when deciding whether an amount of downtime is reasonable the agency will take into consideration the performance of a similarly situated data provider and whether the downtime has resulted in tangible and material harm to consumers.

As written, the proposal invites scrutiny of slight differences in data provider performance that would have no material impact on a consumer's ability to derive useful functionality from a third-party service. Accordingly, the Associations ask for the removal of all performance specification requirements for the developer interface.

3. Access cap prohibition

The proposal states that a data provider must not unreasonably restrict the frequency with which it receives and responds to requests for covered data from an authorized third party. The Associations agree that restrictions on the frequency of requests are reasonable if they are related to risk management concerns under § 1033.321. However, the CFPB should also clarify that restrictions on access frequency are reasonable if they are necessary to avoid impairing the performance of the developer interface for other third parties or consumers.

Such an accommodation would be reasonable in situations where a particular third-party's use of an interface impacts the overall throughput of systems that are designed around particular data volume assumptions, and the effect on system throughput degrades access for other parties. In this context, the CFPB should defer to the reasonable business judgment of data providers

⁴³ Remarks from Secretary of the Treasury Janet L. Yellen on Digital Assets (April 7, 2022), available at <https://home.treasury.gov/news/press-releases/jy0706>.

regarding what constitutes an unreasonable impairment of system performance that would justify imposing an access cap.

The CFPB should also recognize that data providers are likely to incur additional costs if they are not able to manage network traffic to preserve system performance. For data providers that have service contracts for APIs priced according to target performance (i.e., priced to account for volume and frequency of access), the CFPB should not penalize data providers who switch service providers that offer compliant interfaces with lower *maximum* throughput. As discussed later, the CFPB should also provide that a reasonable denial of a third party's access request includes a risk management concern related to interface performance under heavy volume (i.e., frequent batch updates from a large aggregator or individual third party).

4. Security specifications

In general, the Associations agree that the appropriate data security standard for insured depositories who are data providers should be rules issued pursuant to Section 501 of the Gramm-Leach-Bliley Act (GLBA). For credit unions, those rules are the NCUA's regulations under 12 CFR Part 748. For nonbank data providers, the CFPB has proposed an alternative compliance standard: the Safeguards Rule promulgated by the Federal Trade Commission (FTC).

In comparison to the prudential regulators Safeguard Guidelines, the FTC's rule lacks the same degree of detail and rigor that results from prudential supervision. The NCUA's framework for implementing the GLBA's safeguards provisions are not just the codified portions of 12 CFR 748, but also include appendices, letters to credit unions, examination workbooks, and the Federal Financial Institutions Examination Council (FFIEC) IT Handbook as reference material. By comparison, the FTC rule operates more as an outline for developing a written information security program.

The Associations note that the FTC cannot examine institutions under its jurisdiction for compliance with its Safeguards Rule. Given these significant differences, the Associations disagree with the CFPB's decision to characterize the prudential regulators' GLBA framework and the FTC's Safeguards Rule as comparable regulatory regimes. The significant differences between the two approaches are not only relevant in terms of individual compliance burden, but also consumer safety. The proposal would invite nonbank covered persons to provide consumer financial products and services while leveraging new data privileges but would not hold these entities to the same level of data security supervision as credit unions or banks. This outcome invites regulatory arbitrage and undermines the CFPB's intended goal of promoting fair competition.

5. Screen Scraping

The proposal also states that a data provider must not allow a third party to access the data provider's developer interface by using any credentials that a consumer uses to access the consumer interface. While the Associations agree with the overall intent of the proposal, which

is to reduce reliance on screen scraping in favor of more secure, API-based exchange, the CFPB should clarify its intended prohibition on screen scraping.

As written, the proposal only bars a third party from using a consumer's credentials to access a developer interface to scrape covered data. This leaves open the possibility of scraping data accessible through a consumer interface or other online banking portal. The Associations favor a more explicit prohibition on scraping from consumer interfaces but recognize the need for flexibility in situations where a data provider currently has agreements to permit scraping from a known and trusted third party.

The Associations also believe it is appropriate to tailor the data provider's obligations to focus on preventing unauthorized access to the developer interface. Data providers are unable to reliably distinguish between logins from a legitimate consumer versus a third party when consumer credentials are presented. Accordingly, the CFPB should not compel a data provider to police third party scraping outside of the developer interface. However, the CFPB should explore mechanisms to support agency supervision of third parties if the goal is to prohibit all scraping, such as by requiring third parties to identify their traffic with headers or other means.

With respect to screen scraping that occurs by agreement, the CFPB should seek to accommodate arrangements data providers may have with trusted parties who are actively pursuing interface-level integration. This would provide important transitional relief during the due diligence phase as data providers work to establish APIs that meet qualified industry standards but also the particular needs of their partners. This relief would also reflect the reality that credit unions and other financial institutions are not equipped to onboard dozens of third-party accessors simultaneously. While credit unions want to eliminate reliance on consumer credentials for data access purposes, there is also recognition that members want to have continued access to existing data streams as third parties are onboarded.

c. § 1033.321 Interface access

1. Denials Related to Risk Management

The proposal permits a covered data provider to deny a consumer or third party access to an interface based on risk management concerns, provided the denial is "reasonable" according to the criteria set forth in proposed § 1033.321(b). The proposal further states that indicia of a reasonable denial include whether access is denied in adherence with a qualified industry standard related to data security or risk management.

While the Associations appreciate the CFPB's recognition that data providers must have the ability to exercise control over interface access to comply with risk management policies, the proposed framework for determining what is a reasonable denial invites confusion and excessive burden.

More importantly, the denial mechanisms available in § 1033.321 are not a substitute for what is more urgently needed to make the proposed rule feasible: a safe harbor for data providers that grant interface access to a third party who makes representations about their security posture.

2. Indicia of Reasonable Denials

The Associations request clarification that indicia of a reasonable denial include a data provider's application of general risk management practices approved by its functional regulator. As written, the proposal would only grant favorable status to a risk management standard adopted through a qualified industry standard, which is likely to derive from an independent standard setting organization (SSO) consisting of regulated and nonregulated entities. An SSO could adopt a risk management standard that does not adequately align with regulatory requirements.

Credit unions and other regulated financial institutions are expected to address the risk management concerns of their functional regulator. For example, the NCUA has published its own guidance related to managing third-party relationships.⁴⁴ An important component of this guidance is reflected in the following statement about policies and procedures: "[c]redit unions should also establish program limitations to control the pace of program growth and allow time to develop experience with the program."⁴⁵ A credit union mindful of this guidance will want to control the pace of third parties onboarding to a developer interface. Not only is this control necessary to exercise adequate due diligence, but it is also a practical necessity in an environment where numerous third parties may seek independent connections with an individual credit union. Accordingly, the Associations ask the CFPB to acknowledge that a reasonable denial includes one based on an organization's effort to control the pace of interface onboarding.

3. Due Diligence for Every Third Party Not Feasible

The CFPB vastly underestimates the upfront and ongoing costs associated with performing risk assessments for third parties seeking access to consumer data. While the text of the proposed regulation permits a data provider to perform voluntary due diligence even after it receives data security information from a third party, the preamble tells another story. "The CFPB expects that, prior to responding to data requests, most data providers would engage in some reasonable risk management diligence in accordance with proposed Section 1033.321(a) as part of approving third parties to access a developer interface."⁴⁶

The statement suggests that a data provider, regardless of what assurances a third party presents about its security practices, will be expected to engage in some level of due diligence. However, what the scope or extent of such due diligence should be remains unclear. Credit unions that

⁴⁴ See NCUA Supervisor Letter, Evaluating Third Party Relationships, No. 07-01 (October 2007), available at <https://ncua.gov/files/letters-credit-unions/LCU2007-13ENC.pdf>.

⁴⁵ *Id.*

⁴⁶ 88 Fed. Reg. 74823.

currently have arrangements with third party accessors may have agreements addressing security, operational, and financial audits as part of a holistic risk mitigation strategy. It would be impractical to perform this risk mitigation under the proposed rule where the data provider would have to manage due diligence and onboarding for tens, if not hundreds, of direct accessors. This burden is amplified with data aggregators that are operating as accessors on behalf of thousands of third-party accessors. Data providers of any size simply do not have the bandwidth to manage that level of due diligence.

By establishing an expectation for vetting third parties on a case-by-case basis (absent some industry accreditation system), the CFPB's statement in the preamble undercuts the agency's principal rationale for proposing § 1033.321(d)(1), which is "to alleviate the concerns [...] related to the potential burden of vetting on smaller data providers and the potential inefficiency resulting from duplicative vetting."⁴⁷

The CFPB makes no attempt to quantify the costs of performing risk assessments for potentially numerous third parties. Instead, the CFPB looks at the potential cost savings to data aggregators resulting from greater standardization of data access agreements and notes, briefly, that "the costs of establishing data access will be limited to ensuring third party risk management standards are satisfied and reviewing the agreements."⁴⁸ Again, the CFPB does not elaborate on what "reviewing the agreements" entails.

While an accreditation system could potentially alleviate some of the burdens associated with case-by-case vetting, the CFPB would not automatically presume that a denial based on a third party's failure to meet a qualified industry standard is reasonable.

Proposed § 1033.321(c) states that a denial based on such a failure would only be regarded as "indicia" of a reasonable denial. In other words, the CFPB might, at its discretion, determine that a third party should have received data access even if it lacked some form of accreditation. The Associations regard this approach as flawed. Such case-by-case determinations could invite inconsistency in risk management standards between the CFPB and other regulators charged with overseeing the adequacy of credit union information security programs.

Additionally, under the proposed denial framework, the CFPB would need to recognize at least one qualified industry standard pertaining to data security or risk management for any industry-led accreditation system to work. To do so, the CFPB would need to assume a role that has traditionally been filled exclusively by prudential regulators, such as the NCUA.⁴⁹ In this regard, the Associations regard the CFPB's ability to effectively dictate risk management tolerances for

⁴⁷ 88 Fed. Reg. 74821.

⁴⁸ *Id.* at 74849.

⁴⁹ Section 1002(12)(J) of the Dodd-Frank Wall Street Reform and Consumer Protection Act excludes financial institutions' information security safeguards under GLBA § 501(b) from the CFPB's rulemaking, examination, and enforcement authority. See 12 U.S.C. § 5481(12)(J).

credit unions and other depositories as jurisdictional overreach. The CFPB cannot have exclusive say as to whether a credit union's denial of a third party is reasonable or not.

Instead, the CFPB should delegate this function, along with the designation of any data security standard applicable to third parties for the purposes of § 1033.321(b), to an FFIEC subcommittee of prudential regulators that includes the NCUA. The CFPB should not proceed with a final rule until FFIEC agencies can identify an appropriate accreditation standard for judging the adequacy of a third party's data security. However, the CFPB should not assume that the existence of an accreditation standard will be sufficient on its own. In the absence of an accrediting organization or supervision performed by a regulator, data providers will still be left with the untenable burden of having to perform their own risk assessments.

Potentially data aggregators might alleviate some of this burden by adopting a qualified industry standard for third parties that link to data providers through their own platform. However, the use of aggregators would not necessarily prevent third parties from establishing independent links to data providers, necessitating individualized risk assessments.

Considering the impracticality of conducting case-by-case due diligence on a massive scale, and the CFPB's apparent lack of interest in performing an accreditation function, permitting third parties to merely represent that they have adequate data security practices cannot possibly address the liability concern of data providers. In these circumstances, what data providers need most is a safe harbor. Even with a safe harbor, the CFPB should assume greater responsibility for its vision of open banking by performing a necessary role: verifying that third parties are accredited or compliant with a qualified industry standard pertaining to data security. The result should be a portal or database of white-listed third parties that have met these standards. The National Automated Clearing House Association's (NACHA's) third-party access portal is a prime model to consider when developing this system. Furthermore, data providers should then be able to rely on the accuracy of the Bureau's information when authenticating a third-party recipient of consumer financial data and this reliance should serve as a safe harbor from agency action and/or in litigation. While the CFPB should not be the sole authority to determine what an appropriate data security or risk management standard is, it should perform at least this supervisory function.

4. Need for Safe Harbor

The Associations urge the CFPB to adopt a safe harbor for data providers who grant access to third parties who make representations about adequate data security or risk management practices. The CFPB has chosen to ignore industry concern about who will ultimately bear the cost of data breaches and mishandling of data by third parties or other downstream entities. The CFPB has declined to adopt a framework for allocating liability in the event a third party loses or mishandles data. The CFPB's silence on this important aspect of its rule implies that credit unions

will need to avail themselves of judicial resources if they or their members suffer harm from a third party exercising data access privileges the CFPB has granted.

The CFPB is likely aware that most credit unions will not be able to obtain judicial remedies from third parties that have mishandled data. Not only is litigation cost-prohibitive for all but the largest financial institutions, the uncertainty of applying § 1033's novel regulatory framework to state laws addressing data security, privacy, or negligence is likely to frustrate the pursuit of equitable remedies. In cases involving fraud or identity theft, consumers will likely turn to their credit union for redress, even if a third party is ultimately responsible for losing sensitive data. Credit unions have observed this trend in the context of resolving nonbank P2P disputes, where members avail themselves of credit unions' superior customer service channels to obtain reimbursement under Regulation E.⁵⁰

To ensure that credit unions are not disproportionately burdened by the costs of third-party data breaches which result in fraud or member harm, the CFPB must adopt a safe harbor for data providers who transfer data to a third party presenting proper authorization and warranting adequate data security practices. The CFPB should make clear the liability for misuse of data lies with the holder of that data.

The safe harbor should protect a data provider from all claims from consumers and third parties relating to the transfer of covered data.

d. § 1033.331 Responding to requests for information.

1. Responding to requests—access by consumers

The Associations seek clarification regarding the extent to which minors may request covered data, either from consumer interfaces or through arrangements with third parties. Credit unions may choose to offer checking and savings accounts to minors but choose not to offer online or mobile banking to avoid triggering obligations under the Children's Online Privacy Act (COPAA).

The proposed rule would require data providers to offer online consumer interfaces to all consumers, with no exclusion for minors, and respond to requests from consumers without exclusion. The lack of any exception would trigger COPPA's applicability for credit unions that have deliberately structured their account policies to minimize such exposure. The Associations request the CFPB grant an exception under § 1033.331 to preserve existing data provider discretion regarding minors' access to online or mobile banking functionality—including access to interfaces.

⁵⁰ See NAFCU, Letter to CFPB re: Request for Information Regarding Relationship Banking and Customer Service; Docket No. CFPB-2022-0040, 5 (August 22, 2022), *available at* <https://www.nafcub.org/system/files/files/8.22.2022%20Letter%20to%20CFPB%20re%20Relationship%20Banking.pdf>.

2. Responding to requests—access by third parties

The Associations request explicit clarification that data providers are permitted to authenticate consumers through their own systems and interfaces as a preliminary step before granting a third party access to covered data. The preamble acknowledges this prevailing industry practice as acceptable: “[w]here consumers provide their credentials directly to the data provider through such an interface, the data provider would generally receive information sufficient to authenticate the consumer's identity.”⁵¹ However, the CFPB also invites comment on whether consumers should be able to bypass authentication through the data provider.⁵²

The Associations regard any mechanism that bypasses a data provider's authentication procedures as insecure, likely to contribute to greater risk of fraud or identity theft, and unlikely to confer any meaningful benefit on consumers. Nonbank third parties that circumvent a data provider's intended authentication pipeline would present an even greater hazard, particularly in an environment where many of these entities are not supervised or regularly examined.

Additionally, the Associations do not foresee any way for a credit union to fulfill its legal obligation to safeguard member data if the CFPB permits a third party to simply attest that it has properly authenticated the consumer.

3. Responses Not Required

The proposal would not require a data provider to notify a consumer if it has denied a third party request to access covered data. The Associations request clarification that such notification may be optional if the data provider wants to notify the consumer about the particular reason for the denial.

4. Revocation

The proposed rule would permit a data provider to make available to a consumer a reasonable method by which the consumer may revoke any third party's authorization to access all of the consumer's covered data. Under proposed § 1033.331(e), to be reasonable, the revocation method must, at a minimum, be unlikely to interfere with, prevent, or materially discourage consumers' access to or use of the data, including access to and use of the data by an authorized third party.

The Associations recommend the CFPB clarify that a data provider that honors a revocation request as “all or nothing” adopts a reasonable revocation mechanism. Credit unions that have experience granting third parties API access report that access privileges are not conditionally defined at the API level. In other words, the ability to partially revoke access (e.g., for particular types of covered data) is not a feature commonly supported in API architectures. The cost to

⁵¹ See 88 Fed. Reg. 74823.

⁵² See *id.*

reconfigure existing API architecture to support such functionality would incur significant costs as it would implicate the credit union's entire security architecture.

A consumer that wishes to exert more granular control over the type of covered data accessible to third parties by selectively revoking access should direct those requests to the third parties. Third parties are in the best position to honor such requests by simply ceasing requests for revoked data categories. The alternative (and vastly more burdensome approach) of requiring the data provider to build the third party's revocation protocol into its own API would force data providers to subsidize third party compliance systems. The Associations regard this outcome as unfair and unlikely to stimulate competition.

e. § 1033.341 Information about the data provider.

In general, the identification requirements under § 1033.341 do not present the same level of concern as other aspects of the rule. However, the Associations urge the CFPB to adjust requirements related to providing developer interface documentation and responding to troubleshooting requests from third parties.

Credit unions that use service providers to develop compliant interfaces should not be responsible for handling documentation and troubleshooting inquiries. Instead, data providers using a service provider to offer a developer interface should have the option of listing the contact information of their vendor for inquiries related to API documentation and technical support.

Credit unions that develop their own interfaces in-house are not equipped to respond to a large volume of third-party inquiries regarding technical documentation or support requests. To provide such support would necessitate significant new investments in personnel that would degrade the credit union's ability to focus on its core mission: providing affordable financial products and services to its members. The CFPB should clarify that a data provider is not obligated to respond to every technical inquiry it receives from a third party.

f. § 1033.351 Policies and procedures.

In general, the Associations agree that policies and procedures designed to implement data provider requirements must be appropriate to the size, nature, and complexity of the data provider's activities. The Associations' concerns regarding compliance with particular requirements are discussed at length in the preceding sections. With respect to policies that are unique to § 1033.351 the Associations urge the following:

1. Ensuring Accuracy

The proposal would require data providers to adopt policies and procedures designed to ensure that covered data is accurately made available through the data provider's developer interface. The Associations agree that the CFPB should focus on the accuracy of data transmission rather than the underlying data itself. As the CFPB acknowledges, other consumer financial laws and the

Safeguards Guidelines already address a data provider’s general obligation to provide accurate information.

2. Record Keeping

The CFPB should reduce the retention period discussed in § 1033.351(d)(1) from three years to one year for records related to a data provider’s response to a consumer’s or third party’s request for information or a third party’s request to access a developer interface. This would align with the Association’s proposed limits on storing historical data. Furthermore, three years of API data has the potential to generate an enormous data footprint necessitating significant investments in storage capacity, particularly if individual records must include a copy of the data covered in each request. The CFPB should clarify that the records of responses to requests for information or interface access requests should not need to include copies of the transferred data.

3. Records of Denials

The Associations urge the CFPB to clarify that records explaining why a data provider denied a particular request do not need to include the specific risk management conclusions of the data provider. A general identification of the type of denial given (i.e., “risk management”) should be sufficient for the purpose of communicating a notice of denied access to a consumer or third party under §§ 1033.351(b)(2) and (3). Divulging specific risk management information, particularly to an unknown third party that may be compromised or lacking legitimate consumer authorization, could present additional security risks to the data provider.

V. Subpart D

a. **§ 1033.401. Third Party Authorization Procedures**

The Dodd-Frank Act directs personal financial data to be made available to consumers which includes “an agent, trustee, or representative acting on behalf of an individual consumer.”⁵³ The proposed rule defines a third party as “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.”⁵⁴ This unlimited, expansive group of actors is only curtailed by the requirement that the third party “must seek to access covered data from a data provider on behalf of a consumer to provide a product or service the consumer requested.”⁵⁵ A third party is only required to meet three criteria in order to become “authorized”:

1. Provide the consumer with an authorization disclosure;
2. Provide a statement to the consumer in the authorization disclosure certifying that the third party agrees to certain obligations; and

⁵³ See 12 U.S.C. 5481(4).

⁵⁴ See § 1033.131.

⁵⁵ See § 1033.401.

3. Obtain the consumer’s express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing.⁵⁶

First, the requirements to become an authorized third party must clearly require the third party to “provide a **financial** product or service the consumer requested.” The statutory language of § 1033 and the intent of this rulemaking is wholly focused on financial products and all regulatory language must ensure that requirement remains throughout the rule.

Second, the Bureau’s decision to interpret the ability of an agent, trustee, or representative to receive data on behalf of a consumer to mean that an egregiously broad group of persons and firms should have continuous access to a consumer’s personal financial data is well beyond the statutory grant of authority. As not-for-profit cooperatives legally owned by their members, credit unions act in the best interest of their members. Furthermore, credit unions are highly regulated, supervised, and examined entities. The CFPB’s broad interpretation of “third party” captures entities that are not regulated, supervised, or examined at the same level as credit unions. In the absence of comparable legal relationships that credit unions enjoy, these fintechs may not have the same incentive to act in the best interests of their consumers. Therefore, third party access on behalf of a consumer should be limited to instances where there is a legal relationship between the third party and the consumer that necessitates the access.

Third, the responsibility to obtain consumer consent to access covered data is misplaced. The data provider, not the third party, is in the best position to confirm the consumer’s identity as the data provider holds the consumer account and has already implemented account verification and access procedures to verify the consumer’s request. While this requires more of the data provider, it will provide a barrier against bad actors seeking to fraudulently induce the consumer to grant account access. This layer of protection would be bolstered by the Bureau’s database of authorized third parties against which the data provider would cross-check access requests. Moreover, the Bureau should make clear data providers have the right to block the release or terminate access to a consumer’s personal financial data if they suspect foul play.

b. § 1033.411. Authorization Disclosure

The purpose of the authorization disclosure is to “provide consumers with key terms of access so they can make informed decisions about granting third party access to covered data” and to ensure the consumer intended the third party to act on their behalf. We strongly support the ability of a consumer to maintain the rights of access to their personal financial data, but credit unions also have a responsibility to ensure that data remains safe, secure, accurate, and private. Today, bad actors have more tools than ever at their disposal in order to perpetrate schemes against unsuspecting consumers. Director Chopra, himself, has warned about the power of

⁵⁶ *Id.*

generative AI to “simulate human interaction” and its potential to “interfere with human life and perpetrate fraud, crime, and abuse.”⁵⁷ Even if consumers make a deliberate effort to gauge the reputability of third parties seeking permissioned access to financial data, sources of public supervisory information about those entities may be lacking. Not all third parties will be subject to the supervision of a functional regulator. This new open banking universe the CFPB is creating where consumers willingly provide access to their personal financial data to third parties invites these criminals to test the waters.

The proposed authorization disclosure is no guarantee that the consumer is providing informed consent. Without strict filters and guardrails limiting the ability of bad actors to pose as legitimate, authentic third parties, consumers could easily be duped into providing “consent.” We need look no further than the rash of payment app fraud consumers have suffered over the last several years. As stated above, relying on data providers to authenticate third parties is also not a viable alternative to protecting consumers from fraudsters. The final rule must significantly curtail the number of entities that can become third parties and the Bureau must play an active role in authenticating these third parties.

The proposed rule defines the “key terms of access” to include: (1) The name of the third party that will be authorized to access covered data pursuant to the authorization procedures; (2) The name of the data provider that controls or possesses the covered data that the third party seeks to access; (3) A brief description of the product or service that the consumer has requested; (4) A statement that the third party will collect, use, and retain the consumer’s data only for the purpose of providing that product or service to the consumer; (5) The categories of covered data that will be accessed; (6) The certification statement; (7) A description of the revocation mechanism; and (8) The name(s) of any data aggregators that will assist the third party with accessing covered data and a brief description of the services the data aggregator will provide.⁵⁸ The final rule should specifically require the authorization disclosure to include the third party’s legal name and any assumed names for doing business with the consumer, a link to the third party’s website, a description of the data security and privacy standards to which the third party will adhere in relation to the consumer’s data, and contact information for the consumer to use if they believe their data was breached with the third party. The third party must also clearly and precisely disclose to the consumer what information the consumer is authorizing the third party to access—the general categories of information would be insufficient for this disclosure. The consumer is trusting the third party to be a responsible steward of their personal financial information, and this consent cannot truly be obtained without accurate and specific consumer disclosure and authorization.

⁵⁷ See CFPB Director Chopra addresses AI concerns. (Dec 6, 2023), *available at* <https://www.consumerfinance.com/2023/12/06/cfpbs-director-chopra-addresses-potential-for-ai-to-give-enormous-power-to-few/>.

⁵⁸ See § 1033.411.

The authorization disclosure should also require the third party to inform the consumer of the frequency with which they intend to access the consumer's data. The disclosure should specify whether the consumer is authorizing a one-time data transfer, as might be required for an account transfer, or a recurring data pull, as might be used for a budgeting tool. This frequency authorization should also apply to the maximum durational limits for the authorization discussed further below. If the consumer is authorizing a one-time data transfer, the authorization should not extend beyond that transfer. Additionally, the Bureau should be proscriptive with the formatting requirements for the authorization disclosure. The authorization disclosure must use plain language, a clearly readable font size, and should prohibit any extraneous language that could cause consumer confusion or obscure the key terms of access.

c. § 1033.421. Third Party Obligations

1. Prohibition on Secondary Uses of Data

As noted above, credit unions are mission-driven, member-focused, and committed to the financial well-being of their members and their communities. Credit unions act in the best interest of their members and can be trusted with access and use of covered data because of their mission-driven relationships with each of their members. The Bureau must strictly regulate secondary uses of consumer data disclosed to third parties to ensure the data is not improperly used at the expense of the consumer, while permitting secondary uses that drive member benefits. The monetization of data is a thriving industry that will be bolstered by the proliferation of open banking. Therefore, the Associations agree that the sale of consumer data by non-financial institution third parties should remain prohibited. The Associations' concerns regarding the misuse of consumers' data are consistent with that of the Bureau—that insufficiently regulated and supervised third parties will leverage their data access for their own benefit.

However, financial institutions and their affiliates are highly regulated, supervised, and examined institutions that already have all categories of covered data within their control or possession. Financial institutions have a proven track record of protection and respect for sensitive financial data. They should therefore be permitted to obtain consumer authorization for legitimate secondary uses of covered data (such as member budgeting and holistic financial management) when acting as a third party in the context of this rulemaking. The authorization for these secondary uses of data should mirror the authorization disclosure described in § 1033.411. If a consumer can accept a financial institution's stand-alone product or service in the marketplace, then they should be able to opt-in to that same product or service in an open banking context.

This consent-based approach would allow consumers to opt-in or opt-out of having their covered data used for targeted advertising and cross-selling. The adoption of this caveat for secondary uses will provide significant consumer benefits and allow financial institutions and their affiliates to utilize the categories of covered data to offer consumers more competitive products and

services.⁵⁹ It will also allow financial institutions to use covered data to strengthen their relationships with members and add meaningful value to the products and services provided by allowing the development of insights about the members to better serve them, such as using the data to provide the member with personalized “insights” about their linked accounts, such as the savings they could enjoy if they switched accounts. Without these additional authorities for financial institutions, the proposed rule will not catalyze competition and consumers will lose. Given the necessary authorizations, this expansion of the use of covered data will provide consumers with a clear understanding of the scope of the data use and maintain consumers’ ability to sufficiently control their data.

Director Chopra heralds this proposed rule as one that will:

“[A]ccelerate much-needed competition and decentralization in banking and consumer finance by making it easier to switch to a new provider. The Personal Financial Data Rights rule would help address many of the root causes of sticky banking – by giving people more power to walk away from bad service and enabling small community banks and nascent competitors to peel away customers through better products and services with more favorable rates.”⁶⁰

Yet, by calling into question whether credit unions can use covered data to benefit their members by offering “better products and services with more favorable rates,” the proposed rule will not fulfill Director Chopra’s promise.

2. Limitations on the Collection of Covered Data

Under the proposed rule, third parties are required to limit the collection of covered data to what is reasonably necessary to provide the consumer’s requested product or service. This limitation is appropriate for this rulemaking. The Associations are concerned that there is not sufficient oversight and supervision of third parties to ensure they are abiding by this limitation. The implementation of § 1033 must be accompanied by corresponding enhancements to oversight and regulation of nonbank fintechs to prevent serious threats to consumer harm. Moreover, data providers must be empowered to end the third party’s access to the developer interface if the data provider discovers the third party has exceeded the scope of authorized data. Data providers should not be responsible for policing the actions of third parties accessing consumer data, but they should not be prohibited from intervening if bad actions are discovered. This authority for

⁵⁹ The Associations also recommend clarifying that the Proposed Rule shall not alter the Gramm-Leach-Bliley Act’s and Regulation P’s requirements related to financial institutions’ sharing of non-public personal information with their affiliates, service providers (including other financial institutions engaged in joint marketing), and non-affiliated third parties.

⁶⁰ See CFPB Director Chopra addresses proposed rule. (Oct. 19, 2023), *available at* <https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-on-the-proposed-personal-financial-data-rights-rule/>.

data providers should include a safe harbor for data providers who act in good faith to prevent the misuse of consumer data.

The one-year maximum duration of collection of covered data following authorization is appropriate for recurring data requests, but as discussed above, for one-time data transfers, no standing authorization should exist. This is a significant grant of authority to an outside party to view the most sensitive, personal information about a consumer. That authorization must not be taken lightly and the consumer's reaffirmation of the authority on a regular basis is vital to ensuring continued informed consent about the collection.

The final rule should direct the third party to submit the consumer's reauthorization to the data provider by the anniversary of the authorization to maintain access to the developer interface. If the third party fails to meet this deadline, the data provider must be enabled to revoke the third party's access for the consumer's covered data without repercussion. The Bureau must also clarify in the final rule the responsibilities of a data provider upon reauthorization with and without interruption. Is the data provider required to re-authenticate the consumer's authorization prior to continuing access? If the consumer's authorization is revoked due to a failure to renew and an interruption in access, is the data provider permitted to pause the third party's access until the data provider is able to complete the verification and authentication of the new authorization? These answers are critical to protecting the rights of data providers.

3. Accuracy

Credit unions strongly believe that accurate information is essential for consumers to make informed financial decisions and for financial institutions to provide products and services. Existing laws and regulations aim to protect against many of the most serious harms resulting from inaccurate data including the Fair Credit Reporting Act (FCRA) and Regulation V, the Electronic Funds Transfer Act (EFTA) and Regulation E, the Truth in Lending Act (TILA) and Regulation Z, and the Real Estate Settlement Procedures Act (RESPA) and Regulation X among many others. Credit unions undergo regular examinations that ensure strict compliance with all relevant laws and regulations, including those mandating data accuracy. Data accuracy is also key to preserving member trust and maintaining a stellar reputation as a trusted financial partner.

These same responsibilities for accuracy of data must be conveyed to the third party with the data. The need for continued accuracy in data is no less acute when the data resides with a non-financial institution. Therefore, the third party's policies and procedures must hold them to a functionally equivalent standard as data providers and, as a part of the oversight and supervision of the third parties, third parties must be held to account for their compliance with these policies and procedures. The measure of reasonableness for these policies and procedures should be the similarity to the protections provided to the data by financial institutions.

4. Data Security

One of the most significant concerns for credit unions regarding implementation of § 1033 relates to the security of their members' information. Many credit unions worry that members who share login credentials or identifying information with unvetted third parties will be more vulnerable to fraud. One study regarding the relationship between fraud and consumer use of data aggregators suggests that these concerns are not unwarranted; a large Australian bank has reported that "customers with logins via an aggregator are two or more times more likely to experience fraud."⁶¹

While some third parties may be subject to the FTC's enforcement jurisdiction, the FTC's Safeguards Rule is not as comprehensive as the information security standards adopted by federal banking agencies (i.e., the Safeguard Guidelines). Moreover, the FTC does not actively supervise companies for compliance with its own Safeguards Rule.

By contrast, non-public personal information maintained by financial institutions is regulated by the GLBA. The GLBA restricts financial institutions from sharing certain nonpublic customer information as well as requiring them to safeguard the security and confidentiality of customer information.⁶² The GLBA is implemented, in part, by the CFPB's Regulation P, which governs financial institutions' treatment of nonpublic customer information, including the conditions under which they may disclose such information to nonaffiliated third parties.⁶³

In addition, provisions of the GLBA are implemented by the NCUA's part 748, which requires credit unions to maintain security programs for safeguarding customer records and information.⁶⁴ Specifically, credit unions must maintain safeguards to:

- Ensure the security and confidentiality of customer records and information;
- Protect against anticipated threats or hazards to the security or integrity of such records; and
- Protect against unauthorized access to or use of such records or information that would harm or inconvenience a member.

The Federal Financial Institutions Examination Council (FFIEC) has continued to promulgate highly specific guidance to implement the GLBA's safeguards provisions and promote IT security as technology evolves. Furthermore, the FFIEC agencies—including the NCUA—have developed specialized procedures for assessing the security of regulated institutions. Credit unions receive

⁶¹ See Clancy Yeates, "Very concerning correlation: CBA warns against screen scraping," Sydney Morning Herald (March 17, 2020), available at <https://www.smh.com.au/business/banking-and-finance/very-concerningcorrelation-cba-warns-against-screen-scraping-20200316-p54am8.html>.

⁶² 15 U.S.C. §§ 6801-6809.

⁶³ 12 C.F.R. Part 1016.

⁶⁴ 12 C.F.R. Part 748.

regular cybersecurity focused examinations, whereas this may not be the case for every third-party data recipient or data aggregator.

In the absence of a national federal data security standard and national data privacy standards, granting entities who are not subject to substantially similar laws and regulations broad data access privileges would be irresponsible. For this reason, simply requiring third parties to comply with the FTC Safeguards Rule is wholly insufficient. All parties who collect or hold consumers' personal financial data should be held to the same standards. Like the risks to inaccurate data discussed above, the security and privacy risks related to financial data are no less serious when the data is held at a non-depository institution.

The Associations recommend the CFPB adopt the Safeguard Guidelines promulgated by the federal banking agencies and the NCUA as the appropriate standard for third parties rather than the less comprehensive FTC Safeguards Rule. Without the benefit of contractually negotiated terms of data access, variability in data security expectations will only expose consumers to greater risk. Credit unions, as primary account holding institutions, will also bear a disproportionate burden since they will need to guard against potentially numerous downstream externalities associated with a third-party's mishandling of member information.

For credit unions, the ongoing cost of protecting members' financial data is significant since it involves not only the entire IT infrastructure, which supports digital and online banking operations, but also the specific cybersecurity costs associated with mitigating data breaches and security incidents that occur beyond the walls of regulated financial institutions. Credit unions also face examination and compliance costs related to supervision of data security.

Credit unions who have earned the trust of their members by investing in security should not be forced to undermine their efforts by unconditionally accommodating third party access privileges. Adding to this problem, the proposed rule does little to clarify where data security responsibilities begin and end. As a result, allocating the costs of events like data breaches or seeking reimbursement for fraud losses caused by a third party's mishandling of data would be unclear and likely dependent on state law because § 1033 does not address questions of liability or indemnity.

Any data sharing rulemaking must consider the necessity of everyone safeguarding consumer information. Currently, there are regulatory gaps that fintechs and other companies exploit to provide financial services. This leads to less consumer protection and, at its worst, leads to the exploitation of consumers as their expectation of consumer protection has historically been based on the regulation of financial institutions and the products and services they offer. Consumer protection can be vastly different when a product or service is offered by non-financial institutions, and consumers do not always appreciate this difference. Any sharing of information that leads to less protection of credit union members' valuable information --and that leads to

members being less protected or at worst exploited—is not supported by the Associations and our member credit unions.

A not unlikely scenario might involve a third party that experiences a breach involving data it acquired from a data aggregator, who originally sourced the data from a bank or credit union after obtaining permission directly from a consumer. In such a scenario, the credit union might suffer reputational damage, fraud losses or need to pay to reissue credit cards for affected members, even if it bears no responsibility for the breach. The credit union would also potentially face dilution of its claims for damages if other data users and data holders are also affected. Data breach cases such as these are already difficult to resolve under current law.

One mechanism for better allocating data security responsibilities between data providers and recipients would be a national, federal data security and privacy standard. Such a standard should harmonize existing federal data security and privacy laws into a single comprehensive standard, recognize credit unions' existing compliance with the GLBA as the gold standard to which all other actors must be held, fully preempt state data security and privacy laws, and implement proper guardrails for consumers' protection across the entire data ecosystem rather than just certain sectors. The Associations encourage the CFPB to support development of a national data security and privacy standard before issuing a final rule, or else find separate authority to ensure that all third parties are governed by the same standards that apply to credit unions and other federally insured depositories.

5. Provision of Covered Data to Other Third Parties

The conveyance of all obligations regarding the consumer's data from one third party to another is appropriate and necessary in light of the sensitive nature of the data and the potential harm to consumers and data providers that could result from the data's misuse. The final rule should require the primary third party to notify the consumer and the data provider when providing covered data to another third party. This notification should include the secondary third party's: (1) Legal name and any assumed names used for doing business with the consumer; (2) A link to its website; (3) Its Legal Entity Identifier (LEI); (4) Contact information that enables a consumer or the data provider can use to inquire about the third party's data security practices; and (5) The specific reason(s) for providing the secondary third party with the covered data. If for any reason the consumer or data provider objects to the data sharing, the primary third party must immediately cease the data sharing and the secondary third party must no longer use or retain the covered data that was shared.

6. Revocation of Authorization

The Associations support the clear, conspicuous, and easy to operate revocation mechanisms. It is imperative that a consumer be able to easily revoke the third party's access to their personal financial data. The third party's obligations once the consumer invokes the revocation mechanism

must include “prompt” notification to the data provider, data aggregator, and any other third parties to whom the third party has provided the consumer’s covered data of the consumer’s revocation. This notification must be timely and clearly specified in the final rule.

d. § 1033.431. Use of Data Aggregators

The CFPB must ensure that data aggregators and other nonbank data recipients are subject to appropriate supervision before publishing any rule to implement § 1033. Data aggregators play a significant role in terms of facilitating the transfer of consumer data between consumers’ primary account institutions, such as credit unions, and fintech companies. However, data aggregators, which are broadly defined in the proposed rule as entities that are retained by and provide services to the authorized third party to enable access to covered data, are not all subject to the CFPB’s supervisory jurisdiction. While the CFPB has signaled a willingness to invoke dormant authority to improve supervisory oversight of nonbank fintech entities, reliance on case-by-case orders under § 1024(a)(1)(C) of the Dodd-Frank Act does not represent the most efficient path forward—particularly in an environment where growing demand for consumer financial data will likely magnify both the importance and number of data aggregators.

This proposed rule directly implicates the CFPB’s ongoing rulemaking that proposes sweeping changes to the FCRA’s Regulation V. The data sharing requirements proposed under this rulemaking may transform data aggregators that are not currently classified as consumer reporting agencies (CRAs) into CRAs. This classification would require those that provide data to and receive it from CRAs to fully understand and provide input to the Bureau on the combined effects of the proposed rule and Regulation V. Additionally, the CFPB must holistically consider how these rulemakings could impact credit unions as data providers. Neither the proposed rule implementing § 1033 nor the ongoing rulemaking related to the FCRA should result in credit unions being classified as data brokers or CRAs due to their required data sharing responsibilities. Given the significant interplay between these two rulemakings, it is important to obtain stakeholder input on the impact of and intersection between the two rulemakings, and that input cannot be obtained with simultaneous rulemakings. The Bureau must finalize one rulemaking before the impacts on the other rulemaking can be fully understood and explored.

Other fintech firms that meet the proposed rule’s definition of a third party may pose different supervisory challenges. Some companies take advantage of arbitrage strategies to remain outside the Bureau’s supervisory jurisdiction or choose to offer only specialized products designed to evade regulation.⁶⁵ Incidentally, these same strategies may be driving demand for enhanced data exchange to accommodate financial product disaggregation.

⁶⁵ See e.g., CFPB, *Buy Now, Pay Later: Market Trends and Consumer Impacts*, 72 (September 15, 2022) (“[t]he CFPB’s analysis of typical BNPL product features demonstrates that some market participants’ offerings appear to be structured to evade certain federal consumer lending requirements.”), *available at*

Currently, the market largely relies on discrete and contractual relationships by depository institutions to maintain oversight and assess any potential risks to consumers by data aggregators and third parties. This supervisory imbalance creates an unsustainable model as the aggregation services market grows, increasing the risk that the laws applicable to the activities of nonbank participants in this market will be enforced inconsistently. These risks, in turn, raise the prospect that potential consumer harm associated with the activities of third parties will not be timely identified and remedied. Therefore, we believe the highest priority, and a necessary precondition to finalizing data sharing standards, is ensuring that data aggregators and data recipients that are larger participants in the aggregation services market are examined for compliance with applicable federal consumer financial law. We reiterate our call for the CFPB to initiate a larger participant rulemaking.⁶⁶ Without regular and ongoing supervision of larger data aggregators and data recipients, implementation of § 1033 will increase the risk of harm to consumers and competition.

Even for entities that do happen to fall within the Bureau's supervisory jurisdiction, it is questionable whether resources exist to exercise meaningful supervisory oversight. As the Bureau has separately opined, the agency supervises many more nonbanks than it has the capacity to regularly examine. Given that these competitive dynamics already exist, it would be unfair to craft a proposal that perpetuates known supervisory gaps and enables nonbank arbitrage strategies.

The proposed rule makes clear that the obligations and responsibilities of a third party flow through to any data aggregators acting on their behalf. This means that the data providers' authority to end access for third parties due to a violation of the agreement or data security concerns, also extend to the data aggregator acting on the third party's behalf. Data providers must have a safe harbor from negative actions if they are forced to end access for a data aggregator. The data provider must also be provided a grace period for initiating an alternative means of access for the third party(ies) relying on the data aggregator.

https://files.consumerfinance.gov/f/documents/cfpb_buy-now-pay-later-market-trends-consumerimpacts_report_2022-09.pdf.

⁶⁶ See Joint Trades Letter to CFPB re: Petition for rulemaking defining larger participants of the aggregation services market (August 2, 2022).

VI. Conclusion


On behalf of America's credit unions and their more than 138 million members, the Associations urge the CFPB to postpone this rulemaking until critical flaws are addressed and better data can be collected. As proposed, the CFPB's blueprint for open banking will unfairly distort competition and erode the relationship banking model that has underpinned credit unions' cooperative mission. Credit unions cannot afford to subsidize the development, maintenance, and ongoing risk management of an API-based ecosystem that benefits fintech companies, particularly if the CFPB is unwilling to promptly recognize standards or offer safe harbor protections to data providers. Additionally, the CFPB cannot realistically expect credit unions to comply with the proposal within the timeframes given. Not only are extensions of the proposed compliance dates necessary to account for vendor readiness and alleviate implementation bottlenecks, additional exemptive relief is also needed.

Small, mission-focused credit unions lack the resources necessary to subsidize fintech data access and diverting scarce resources to API development or fintech risk management will harm the quality of member service. CFPB rules that tilt the playing field in favor of technology focused companies, as opposed to those that are actually accountable to the communities they serve, like credit unions, will erode the foundation of main street community financial services. Accordingly, the Associations urge the CFPB to pause this rulemaking and consider substantial changes to the proposal.

The Associations appreciate the opportunity to submit comments in response to the CFPB's proposed rule. Should you have any questions or concerns, please do not hesitate to contact either Andrew Morris at amorris@nafcu.org or Madison Rose at mrose@cuna.coop.



Madison Rose
Credit Union National Association
Senior Director of Advocacy & Counsel



Andrew Morris
National Association of Federally-Insured Credit Unions
Senior Counsel for Research and Policy