Credit Union National Association
CUNA

Washington, D.C.
99 M Street SE, Suite 300
Washington, D.C. 20003-3799
Phone: 202-638-5777
Toll-Free: 800-356-9655

January 25, 2023

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

Re: Outline of Proposals and Alternatives Under Consideration for Required Rulemaking on Personal Financial Data Rights

Dear Director Chopra,

The Credit Union National Association (CUNA) represents America's credit unions and their more than 130 million members. On behalf of our members, we are writing regarding the Consumer Financial Protection Bureau's (CFPB or Bureau) Outline of Proposals and Alternatives Under Consideration (Outline) for the Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights[1] implementing Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (§ 1033).[2]

Credit unions are committed to the financial well-being of their members and their communities. As not-for-profit, democratically controlled depository institutions, credit unions deliver big financial and nonfinancial benefits to their member-owners. Data shows that, on average, credit union members are more financially resilient than other consumers. Credit union members are also significantly more likely than nonmembers to use financial education and counseling services. This means that credit union members are more likely to engage in practices that improve their financial well-being and report that the financial institution they own has improved their financial well-being.

This dedication to credit union members includes ensuring their members maintain the rights of access to their personal financial data and that the information remains safe, secure, accurate, and private. With this in mind, we ask the Bureau to consider the recommendations delineated below when designing the rules to foster innovation and improve the lives of consumers.

[1] https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf
[2] 124 Stat. 2008 (codified at 12 U.S.C. § 5533).

I. Third-party Access

a. Qualification as an Authorized Third Party

The Dodd-Frank Act directs personal financial data information to be made available to consumers which includes "an agent, trustee, or representative acting on behalf of an individual consumer."[3] The Bureau's Outline contemplates that data recipients and data aggregators could serve as third party recipients of consumer's personal financial data[4] under this definition. Data recipients are defined as third parties that utilize consumer data to provide: "(1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer."[5] Data aggregators are considered entities supporting data recipients and providers in "enabling authorized information access."[6] Under the Outline's proposal, these groups are only required to meet three criteria:

1. Provide the consumer an "authorized disclosure" soliciting the consumer's informed consent to certain disclosed key terms of access;
2. Obtain the consumer's express consent; and
3. Certify that it will abide by certain obligations regarding its collection, use, and retention of consumer information accessed under the rule.[7]

Once the third party presents this information to the covered data provider, the onus is on the covered data provider to authenticate the third party's identity. This burden is entirely too heavy, especially for small credit unions lacking the manpower or funding to verify each request. Instead, the Bureau should take ownership of authenticating third parties and provide covered data providers with a list or database of verified third parties that are deemed qualified and authenticated by the Bureau. As the federal regulator leading the rulemaking process, the CFPB is uniquely positioned to gather, compile, and analyze the necessary information from data recipients and data aggregators to validate their legitimacy and protect consumers from fraudulent access attempts. The National Automated Clearing House Association's (NACHA's) third-party access portal is a prime model to consider when developing this system. Furthermore, covered data providers will 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.

As a part of the authorization disclosure, the third party would provide key scope and use terms to the consumer. The Outline proposes these terms would include: "general categories of information to be accessed, the identity of the covered data provider and accounts to be accessed, terms related to duration and frequency of access, how to revoke access, the identity of intended data recipients and data aggregators to whom the information may be disclosed, and the purpose for accessing the information."[8] The scope and use terms require much more specificity. The third party must clearly and precisely disclose to the consumer exactly what information the consumer is authorizing the

[3] *See* 12 U.S.C. 5481(4).
[4] Outline, pg. 5.
[5] *Id*.
[6] *Id.*
[7] *Id* at 36.
[8] *Id* at 16.

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. Additionally, the identities of the intended recipients of the data must be completely and truthfully disclosed to the consumer by including any "doing business as" names.

b. Consumer Consent for Access

The Outline proposes the third party should be responsible for obtaining the consumer's consent to access personal financial data under the rule.[9] This responsibility is misplaced. The covered data provider 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 may slightly increase the burden on 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 covered data provider would cross-check access requests. Moreover, the Bureau should make clear covered data providers have the right to block the release or terminate access to a consumer's personal financial data if they suspect foul play.

c. Accuracy of Information Provided to Consumers and Third Parties

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. The Bureau has proposed the following approaches "to ensure that covered data providers transmit consumer information accurately":

1. Require a covered data provider to implement reasonable policies and procedures to ensure that the transmission of information through the covered data provider's third-party access portal does not introduce inaccuracies;
2. Establish performance standards relating to the accurate transmission of consumer information through third-party access portals;
3. Prohibit covered data provider conduct that would adversely affect the accurate transmission of consumer information; or
4. Require a combination of (1) through (3).[10]

These approaches would be both burdensome and duplicative in light of existing data accuracy

[9] *Id* at 15.
[10] *Id* at 34.

and dispute resolution laws and regulations.

d. Secondary Uses of Consumer Data

The Bureau must strictly regulate and curtail secondary uses of consumer data disclosed to third parties to ensure usage for only those disclosed and agreed to by the consumer and for compliance with other laws and regulations relating to the provision of products and services. The monetization of data is a thriving industry that will be bolstered by the implantation of this data sharing. The authorization disclosure provided to consumers must clearly and fully disclose all uses—both primary and secondary—for the data. Any secondary sale of consumers' personal financial data should be subject to an opt-in provision.

II. Data to be Made Available Under the Rule

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.

a. Periodic statement information for settled transactions and deposits.

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

b. Information regarding prior transactions and deposits that have not yet settled.

This category of information is generally consistent with information currently provided to credit union members as well as the scope of the § 1033(a). When credit unions display this information on online banking platforms, the transactions are clearly labeled as "pending" or "not yet settled" so it is clear to the member that the amount of these transactions may change. This clarity must be maintained when third parties utilize this category of information to provide products and services to consumers.

c. Other information about prior transactions not typically shown on periodic statements or portals.

Information about prior transactions not typically shown on periodic statements or portals should be excluded from the rule or at least significantly curtailed. Not only would the inclusion of this category of information impose a heavy burden on credit unions but it could increase the risk of fraud for consumers.

When discussing this category, the Outline describes information such as "the interbank routing of a transaction" and "the name and account number at that bank of the merchant or other payee (such as a fraudster) that deposited the payment transaction" to help consumers recover in cases of fraud or erroneous payments. Credit unions strongly support efforts to stop fraudulent schemes and work diligently to help their member-owners recover when they fall victim to fraud or unauthorized payments, but the required disclosure of confidential account information with largely unregulated, unsupervised third parties is misguided.

If the final rule includes this category of information, it should absolutely not include name and account information for payees, and any information included should be narrowly tailored to have a clear and demonstrable purpose that limits the burden on small financial institutions.

d. Online banking transactions that the consumer has set up but that have not yet occurred.

The value of this category of information is unclear given the general operational procedures for scheduled bill payments: both one-time and recurring. The Outline discussion envisions a consumer entering these payments into the system of their covered data provider (such as their financial institution's online banking platform) 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 covered data provider's platform, the provider will often not know in advance the amount of the bill. The Bureau should limit this category to a list of entities with whom the consumer has scheduled transactions.

e. Account identity information.

Under no circumstances should this category of information be included in the rule. Account identity information is strictly confidential because of the significant risks of fraud, security breaches, privacy breaches, misuse of information and other significant consumer protection risks that come with disclosure of this information. Furthermore, the disclosure of demographic information about consumers invites serious concerns regarding the use of this data for third parties providing products and services to consumers and potential discriminatory actions by these third parties.

The CFPB proposes account identity information could be utilized for account verification in the authorization process. This usage would be unnecessary if the Bureau were to shift

the liability for obtaining consumer consent to access the information to the covered data provider. Any additional need for account identity information could be met by the consumer providing the information directly to the third party.

f. Other information (consumer reports from consumer reporting agencies obtained and used by the covered data provider in deciding whether to provide an account or other financial product or service; fees that the covered data provider assesses in connection with its covered accounts; bonuses, rewards, discounts, or other incentives that the provider issues to consumers; and information about security breaches that exposed a consumer's identity or financial information).

This category of miscellaneous information appears to largely exceed the bounds of the statutory language of § 1033(a) because it is not information pertaining to a product or service; however, fees assessed in connection with a covered account are within the scope of the statute and should be included as a sharable data point. The Bureau must re-evaluate whether the disclosure of alternative data points contained in this section is prohibited under various federal and state laws as well as contractual terms.

Dodd Frank § 1033(a) also sets forth four exceptions to the disclosure requirement:

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 if a rule develops 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 invention, monitoring, and control of data, the incentive to create and allow access to data will reduce. Free riding prevents the production and consumption of goods and services through conventional free- market methods. To the free rider, there is little incentive to contribute to a collective resource since they can enjoy its benefits even if they don't. As a consequence, the producer of the resource cannot be sufficiently compensated. The shared resource must be subsidized in some other way, or it will not be created.

To counteract the free-rider problem and to protect consumers, these exceptions must be interpreted with a broad stroke. The Outline's analysis of these exceptions displays an intent by the Bureau to adopt the narrowest interpretation of these exceptions. 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.

III. Third-party Access Portal

The Outline provides that a covered data provider would be *required* to make information available to third parties once the required authorizations have been provided. The Bureau provides two methods to accomplish this sharing: (1) through authorized access that uses proprietary software to convert consumer data presented in the provider's online financial account management portal into standardized machine-readable data through screen scraping, using a consumer's credentials; or (2) through a portal based on a data-sharing agreement that third parties can access without possessing or retaining a consumer's credentials.

Credit unions have expressed opposition to screen scraping due to the impact on system operability and member access to their accounts through digital platforms. Additional concerns have been raised about the possibility for unauthorized access, the inability to limit the scope of access once the third party enters the system, and data privacy and security worries with this method. These concerns apply to both credential-based and tokenized screen scraping methods. Credit unions also have concerns about the cost, technological feasibility, and upkeep of creating a third-party access portal through an API but largely view this as the preferable option.

A. Cost and Timeline

One of the most common refrains heard from credit unions when discussing this proposal is that the cost estimates and timelines for implementation presented by the Bureau are vastly understated for this type of endeavor. There will be direct costs to covered data providers for allowing access to consumers or third parties as well as ongoing costs for system upkeep, staff allocations, and customer service matters. For credit unions, most internal systems that house consumer data were not designed to share data with outside parties at the request of a member or on an ad hoc basis. Furthermore, the industry cannot allow direct access without major modifications or replacements of current systems, which are costly. Although most credit unions are able to grant third party access for processing and delivery of services, these processes are part of the core functional design of core operating systems and are certainly not designed to provide the type of third-party access to the wide range of information envisioned by this Outline.

Credit unions are member-owned, so any costs associated with section 1033 requirements will accrue directly to the member-owners, i.e., consumers. Any new requirements under section 1033 should consider the impact on financial institutions with respect to size and sophistication as well as the ability to fulfill its 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. This ongoing burden can be lessened by direct access methods; however, such solutions require significant upfront implementation costs and will likely accrue to the further benefit of larger institutions.

Credit unions, system partners, and core providers are currently unable to provide exact timelines or cost estimates because they do not have a clear proposal. The Bureau should collaborate with core providers and credit unions to develop clear time and cost estimates for building and implementing the API and present that information for consideration and evaluation of impact and feasibility. The CFPB is designing the rule and is uniquely positioned to provide these parties with the nuanced information needed to produce a viable proposal.

Director Chopra has indicated he plans to finalize this rulemaking on an accelerated timeline. Given the seriousness of the proposals under consideration, their potential to transform the financial services system, and the unknown and complicated undertaking this will be to create, the Bureau must provide an extended implementation timeline for this rulemaking. Credit unions must be provided with sufficient time to

develop, implement, and test APIs. Further timelines for compliance must be commensurate with the size and complexity of the institution. The impact to the safety and security of consumer data if the development of this portal is rushed could be catastrophic.

B. Unfair Allocation of Costs and Burden

Far too much of the burden for developing, implementing, and maintaining these systems falls on the covered data provider. For example, the third-party portal availability factors place responsibility directly on the data provider:

- The general reliability of a third-party access portal in response to electronic requests to the portal for information by an authorized third party;
- The length of time between the submission of a call to a third-party access portal and a response;
- System maintenance and development that involve both planned interruptions of data availability and responses to unplanned interruptions;
- Responses to notifications of errors from an authorized third party; and
- Limitations or restrictions on fulfilling a call from an authorized third party even when data are otherwise available.

The third parties are deriving significant benefit from the investment of time, money, and continued upkeep that covered data providers are sinking into this system with little or no cost for the third party. If third parties can access and use this data without paying their fair share, these third parties are free-riders. Without a careful allocation of costs of invention, monitoring, and control of data, the incentive to create and allow access to data will reduce. Free riding prevents the production and consumption of goods and services through conventional free- market methods. To the free rider, there is little incentive to contribute to a collective resource since they can enjoy its benefits even if they don't. As a consequence, the producer of the resource cannot be sufficiently compensated. The shared resource must be subsidized in some other way, or it will not be created.

IV. Data Security and Privacy

Non-public personal information maintained by financial institutions is regulated by the Gramm-Leach-Bliley Act (GLBA). GLBA restricts financial institutions from sharing certain nonpublic customer information as well as requiring them to safeguard the security and confidentiality of customer information.[11] 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.[12]

In addition, provisions of the GLBA are implemented by the National Credit Union Administration's (NCUA) part 748, which requires credit unions to maintain security programs for safeguarding customer records and information.[13] 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.

[11] 15 U.S.C. §§ 6801-6809.
[12] 12 C.F.R. Part 1016.
[13] 12 C.F.R. Part 748.

In theory, third parties fit GLBA's definition of financial institution,[14] and thus should be subject to the requirements of GLBA. However, the GLBA's circuitous definitions make it difficult for businesses to always arrive at this conclusion.[15] Third parties that don't usually consider themselves "financial institutions" would benefit from a regulation that clearly establishes the scope of the GLBA and clarifies that these data users would be subject to Regulation P and the FTC's Safeguards Rule.[16]

Additionally, the cybersecurity environment has become increasingly difficult to control. CUNA supports credit union members' and consumers' ability to access and share their financial data in a secure, transparent manner, while ensuring that they fully understand the implications of sharing data. However, there are high risks to consumers, institutions, and society if financial data is not effectively safeguarded.

Identity theft costs continue to increase. In 2016, an estimated 10% of persons age 16 or older reported that they had been victims of identity theft during the prior 12 months. The portion of the population that experienced identity theft increased from 7% in 2014 to 10% in 2016. An estimated 12% of identity-theft victims had out-of-pocket losses of $1 or more; 88% either had no out-of-pocket losses or losses of less than $1. According to the 17.7 million persons age 16 or older who experienced one or more incidents of identity theft with known losses of $1 or more, total losses across all incidents of identity theft totaled $17.5 billion in 2016.

Similarly, Symantec data shows that 4,818 unique websites were compromised with form jacking code every month in 2018. With data from a single credit card being sold for up to $45 on underground markets, just 10 credit cards stolen from compromised websites could result in a yield of up to $2.2 million for cyber criminals each month. The appeal of form jacking for cyber criminals is clear.

Therefore, any data sharing rulemaking must consider the necessity of everyone safeguarding consumer information. Currently, there are regulatory gaps that fintech 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 CUNA and our member credit unions.

V. Liability Shifting

While credit unions are subject to numerous requirements regarding the treatment and safeguarding of their members' nonpublic financial information, many third parties are not subject to similar requirements. This is particularly of concern in light of the CFPB's current focus on expanding third-party access to consumers' financial information. For example, credit unions and banks have a long history of protecting consumers'

[14] *See* 15 U.S.C. § 6809(3) defining "financial institution," which is "any institution the business of which is engaging in financial activities as described in [the Bank Holding Company Act of 1956, § 4(k).]" as interpreted by the Board of Governors of the Federal Reserve to encompass any entity that provides data processing, data storage, and data transmission. 12 U.S.C. § 1843(k).

[15] The term "financial institution" means any institution the business of which is engaging in financial activities as described in § 1843(k) of title 12 [the Bank Holding Company Act]." In turn, 12 U.S.C. § 1843(k) includes as a "financial institution," any company that is "engaging in activities that are financial in nature," as defined by regulation. The United States Department of Treasury defined by regulation pursuant to 12 U.S.C. § 1843(k) such "financial" activities at 12 C.F.R. 225.28(b).

[16] 16 C.F.R. § 314.3.

most cherished physical assets with vaults and safe deposit boxes. Credit unions protect monetary balances from theft, as the government provides business certainty through safety and soundness regulations and deposit insurance. This long history of trust has been developed over time but will be at serious risk through implementation of section 1033 without a parallel focus on protecting consumers' data and privacy.

While criminals profit from cyber theft, the financial institutions who are victims of cybercriminal attacks must pay the cost of the losses. For example, the Truth in Lending Act requires credit card issuing credit unions and banks to bear the cost of unauthorized use.[17] Further, if card issuers refuse to cover these costs, consumers can hold the credit union or bank liable.[18] In addition, private class action attorneys are extracting millions of dollars from companies by applying a standard that anything less than perfect protection is actionable.[19]

Another consideration is that presently, data owners, such as credit unions, have limited legal options when once-trusted service providers lose, abscond with, or misuse credit union data. While the Gramm-Leach-Bliley Act requires the "financial institution" and "non-affiliated third parties" to safeguard data,[20] the statute does not provide financial institutions with private rights of action or statutory penalties to hold third parties accountable in the event of a data loss or misuse. Consumer data is protected only to the extent of its owner's contract rights. Only regulatory agencies can enforce the GLBA provisions.[21] This leaves financial institutions between a rock and a hard place: if a third party errs with the data, the financial institution can be held responsible, but it has only limited contract remedies to place the responsibility where it belongs.

The strict regulation of the delivery of financial services at the federal, state, and local levels should not change simply because unregulated entities seek to provide services that are subject to strict regulation when delivered by a financial institution or other regulated entity. Accordingly, CUNA urges the Bureau to provide actionable remedies for financial institutions against the criminals who steal data or third parties that lose or misuse data. And it certainly includes requiring all financial data users to play by the same rules.

The rules should unambiguously shift liability from a covered data provider to a third party when the data leaves the data provider's system. As more personal information is disclosed in the ecosystem, the opportunities for bad actors to misuse the data grows exponentially. Therefore, not only should the Bureau design a rule that mandates data security and privacy regulations and oversight for third parties, but the CFPB should make clear the liability for misuse of data lies with the holder of that data. Furthermore, the duty to comply with breach notification standards should lie with the entity where the breach occurred. Covered data providers are often the trusted financial partner of consumers and the first call when their data is compromised in any way. While the credit union will go above and beyond to assist their members, the liability and fault must be properly assigned.

---

[17] 15 U.S.C. §§ 1666–1666j.

[18] TILA provides a private right of action, 15 U.S.C. § 1640(a), to all "consumers who suffer damages as a result of a creditor's failure to comply with TILA's provisions." Household Credit Servs., Inc. v. Pfennig, 541 U.S. 232, 235, 124 S. Ct. 1741, 158 L.Ed.2d 450 (2004). Section 1640(a) permits recovery of actual damages, statutory damages, costs, and attorneys' fees, and, as relevant here, may be used as a basis for a claim against "any creditor who fails to comply with any requirement imposed under [15 U.S.C. §§ 1631– 1651], including any requirement under ... [15 U.S.C. §§ 1666–1666j]." Ramadan v. Chase Manhattan Corp., 156 F.3d 499, 502 (3d Cir. 1998).

[19] Legal theories include negligence; breach of contract; fraud; unfair, deceptive, or abusive acts or practices (UDAAP) laws; violation of consumer protection statutes; violation of the Stored Communications Act (SCA); breach of duty; and invasion of rights to privacy.

[20] 12 U.S.C. § 6802(c).

[21] 12 U.S.C. § 6805.

VI. Petition for Rulemaking Defining Larger Participants of the Aggregation Services Market

As noted in our Petition for Rulemaking Defining Larger Participants of the Aggregation Services Market,[22] the Bureau must cultivate a level playing field among all businesses operating in the personal financial data sharing ecosystem. Currently, only highly regulated financial institutions such as banks and credit unions are examined regularly by the CFPB and/or the prudential regulators for compliance with regulations and agency guidance. Instead, 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 data recipients. 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 ensuing 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. Without regular and ongoing supervision of larger data aggregators and data recipients, implementation of Section 1033 will increase the risk of harm to consumers and competition.

Conclusion

On behalf of America's credit unions and their more than 130 million members, we thank you for the opportunity to share our views with the CFPB regarding the Outline. If you have questions or require additional information related to our feedback, please do not hesitate to contact me at (202) 577-3463 or mrose@cuna.coop.

Sincerely,

Madison Rose
Director of Advocacy & Counsel for Payments and Technology

[22] *See* Joint Trades' Petition for rulemaking defining larger participants of the aggregation services market, available at https://www.regulations.gov/document/CFPB-2022-0053-0001.